ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
“ΨΗΦΙΑΚΕΣ ΕΠΙΚΟΙΝΩΝΙΕΣ ΔΕΔΟΜΕΝΩΝ”

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ - ΤΜΗΜΑ ΔΙΔΑΚΤΙΚΗΣ ΤΕΧΝΟΛΟΓΙΑΣ & ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΤΙΤΛΟΣ

Ανάλυση του Εργαλείου CRAMM

Διπλωματική εργασία του Χλη Καλογερόπουλου Ηλία

Ευχαριστίες

Ευχαριστώ πολύ τον καθηγητή μου κύριο Λαμπρινουδάκη Κώστα για την ιδέα εκπόνησης της εργασίας αυτής και την πολύτιμη βοήθεια του καθ' όλη την διάρκεια της συγγραφής της, καθώς και όλους τους καθηγητές που με εφοδίασαν με τις απαραίτητες γνώσεις καθ' όλη τη διάρκεια των σπουδών μου. Επίσης ευχαριστώ την οικογένειά μου , όλους τους φίλους και συναδέλφους μου για την βοήθεια και συμπαράσταση τους.

Σύνοψη

Στην σημερινή εποχή , όπου το κύριο χαρακτηριστικό της είναι η ραγδαία άνθιση της τεχνολογίας , πρωταρχική ανάγκη για την βιωσιμότητα κάθε επιχείρησης είναι η ύπαρξη των πληροφοριακών συστημάτων. Η πολυπλοκότητα αυτών και η ευρύτητα των λειτουργιών τους δημιουργεί την ανάγκη της λεπτομερής ανάλυσης τους σε όλους τους τομείς που συμβάλουν έναν υγιή οργανισμό – εταιρία, επομένως και η βαρύτητα της ασφάλειάς τους , είναι κατανοητό , πως έχει καθοριστικό ρόλο.

Η παρούσα διπλωματική εργασία εκπονήθηκε στα πλαίσια των μεταπτυχιακών σπουδών "Ψηφιακές Επικοινωνίες Δεδομένων" του τμήματος "Διδακτική της τεχνολογίας & Ψηφιακών συστημάτων " Πανεπιστημίου Πειραιώς και ασχολήθηκε πάνω στη μελέτη της ασφάλειας ενός υπαρκτού πληροφοριακού συστήματος μιας εταιρίας στην Ελλάδα. Αυτή η μελέτη έγινε βασισμένη πάνω στα πρότυπα ενός αγγλικού προγράμματος , το ονομαζόμενο "CRAMM" . Το πρόγραμμα αυτό χρησιμοποιείται για τη διευκόλυνση της μελέτης της ασφάλειας σε ένα πληροφοριακό σύστημα. Απαιτεί την συλλογή των επιθυμητών δεδομένων του κάθε αναλυτή – μελετητή , ώστε να προβεί στους κατάλληλους υπολογισμούς και να εξάγει μια καθαρή εικόνα για το πληροφοριακό σύστημα και την ασφάλειά του. Ως ένα γενικότερο σκοπό αυτού , είναι η εμφάνιση των αδυναμιών των πληροφοριακών συστημάτων , η κατηγοριοποίηση και βαθμολόγηση αυτών πάνω σε μια κλίμακα , και οι τρόποι αντιμετώπισης των ήδη υπάρχων κενών ασφαλείας αλλά και μελλοντικών πιθανών κινδύνων. Βέβαια το εργαλείο αυτό μπορεί να χρησιμοποιηθεί και για την μελέτη συγκεκριμένων στοιχείων του συστήματος, επικεντρώνοντας την προσοχή του σε ένα μέρος των λειτουργιών του, πράγμα το οποίο θέλει ιδιαίτερη προσοχή από τον μελετητή.

Η συγκεκριμένη μελέτη επικεντρώνεται στον βασικό κορμό των λειτουργιών του πληροφοριακού συστήματος της εταιρίας με σκοπό την εύρεση των αδυναμιών του, την επεξήγησή αυτών αλλά και την αντιμετώπιση τους. Αυτό υλοποιήθηκε μέσα από την καθοδήγηση των διαδρομών, των επιλογών και μεθοδολογιών που διαθέτει η CRAMM.

Περιεχόμενα

ΘΕΩΡΗΤΙΚΟ ΜΕΡΟΣ

ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

1 ΚΙΝΔΥΝΟΙ & ΣΗΜΑΣΙΑ ΤΗΣ ΑΝΑΛΥΣΗΣ ΤΩΝ ΚΙΝΔΥΝΩΝ

1.1 Εισαγωγή

Στις μέρες μας, η ανάγκη και η χρήση των πληροφοριακών συστημάτων είναι δεδομένη για κάθε οργανισμό / επιχείρηση . Η τεχνολογική πρόοδος που έχει σημειωθεί στην ανάπτυξη των ηλεκτρονικών συστημάτων, η συνδεσιμότητα αυτών, η ελεύθερη ροή πληροφοριών, οι ευκολίες που παρέχει το Internet καθώς και το ηλεκτρονικό εμπόριο έχουν ωθήσει από τις μεγάλες πολυεθνικές εταιρίες και κρατικούς οργανισμούς μέχρι και τις μικρότερες επιχειρήσεις να επενδύουν στην χρήση πληροφοριακών συστημάτων και διαδικτυακών εφαρμογών. Η αναγκαιότητα της χρήσης των πληροφοριακών συστημάτων για την επίτευξη των στόχων και της βασικής λειτουργικότητας τους είναι πλέον γεγονός. Η βιωσιμότητα όλων των επιχειρήσεων είναι συνυφασμένη με την άνθηση και εξέλιξη της τεχνολογίας. Συνεπώς οποιαδήποτε δυσλειτουργία, διακοπή ή είσοδος χωρίς δικαιοδοσία στα συστήματα αυτά συνεπάγεται σε κίνδυνο που αποφέρει πιθανό ενδεχόμενο κόστους, είτε αυτό γίνεται από άμεσες οικονομικές απώλειες, είτε από την αδυναμία του κάθε οργανισμού να λειτουργήσει αποδοτικά, είτε από κλοπή πληροφοριών.

Πέρα από τις οικονομικές επιπτώσεις που μπορεί να υπάρχουν στις επιχειρήσεις πρέπει να σημειωθεί πως τα προβλήματα ασφαλείας των πληροφοριακών συστημάτων γίνονται ακόμα πιο κρίσιμα και αισθητά σε συστήματα που είτε περιέχουν ευαίσθητα δεδομένα είτε επιτελούν και επεξεργάζονται ευαίσθητες και σημαντικές λειτουργίες όπως συστήματα με απόρρητα στρατιωτικά , ευαίσθητα ιατρικά και προσωπικά δεδομένα , σύστημα ελέγχου εναέριας κυκλοφορίας κτλ.

Είναι λοιπόν κατανοητό πως η πιθανή ρήξη της ασφάλειας τέτοιων πληροφοριακών συστημάτων μπορεί να προκαλέσει σοβαρότατα προβλήματα που απειλούν άμεσα αλλά και έμμεσα ανθρώπινες ζωές καθώς και την ασφάλεια τοπικού, εθνικού και παγκόσμιου επίπεδου. Η ασφάλεια των πληροφοριακών συστημάτων και η τεράστια σημασία τους στην σύγχρονη κοινωνία πρέπει να παίζει πρωτεύον ρόλο κατά την σχεδίαση, συντήρηση και χρήση τους.[8]

1.2 Ιστορική αναδρομή στα προβλήματα ασφάλειας

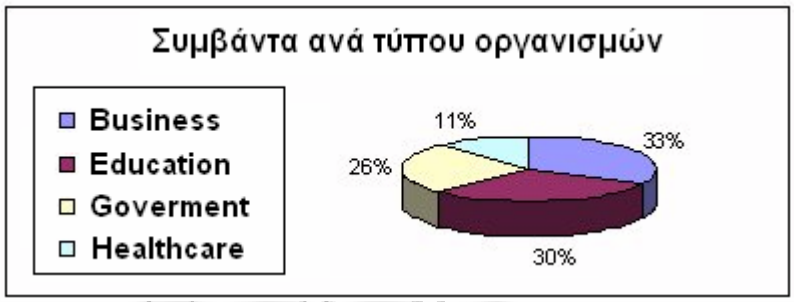
Πριν από μερικές δεκαετίες, τα πληροφοριακά συστήματα άρχισαν να εμφανίζονται και να διεισδύουν σε μεγάλες κυρίως επιχειρήσεις. Τα φαινόμενα παραβίασης αυτών ήταν σχεδόν ανύπαρκτα καθώς λίγοι ήταν αυτοί που γνώριζαν την συγκεκριμένη τεχνολογία και που μπορούσαν να τα χειριστούν. Κατά την διάρκεια των επόμενων δεκαετιών οι νέες τεχνολογίες οδήγησαν σε ευρεία χρήση των ηλεκτρονικών υπολογιστών μεγαλώνοντας ραγδαία τον αριθμό των ανθρώπων που είχε τη γνώση και τα χρησιμοποιούσε, με αποτέλεσμα το πλήθος των παραβιάσεων ασφαλείας να ακολουθεί μια συνεχή αύξηση.

Η ταχύτητα ανάπτυξης της επιστήμης της πληροφορικής ανάγκασε τις εταιρίες ανάπτυξης λογισμικού και προϊόντων πληροφορικής να παράγουν προϊόντα στην αγορά στον ελάχιστο δυνατό χρόνο , χωρίς να δίνουν σημασία στις ευπάθειες και τους κινδύνους που μπορεί να εμφανίζουν είτε λόγο άγνοιας αυτών είτε λόγο πίεσης χρόνου. Έτσι πολλά από τα προϊόντα αυτά περιείχαν λάθη στην υλοποίηση τους τα λεγόμενα bugs.

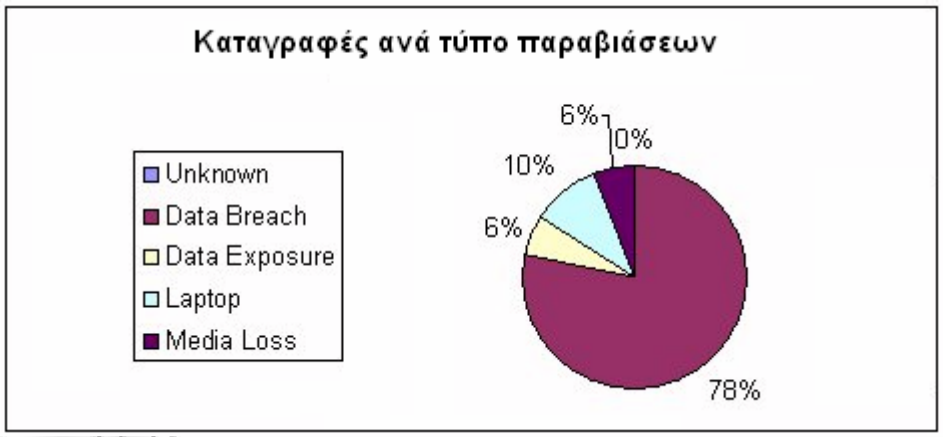
Παρόμοια σφάλματα βέβαια κάνουν και οι εταιρίες που χρησιμοποιούν τα υπολογιστικά συστήματα για την εσωτερική τους λειτουργία. Για λόγους κόστους, χρόνου αλλά και άγνοιας σε θέματα ασφαλείας, παραβλέπουν την ασφάλεια κατά την εγκατάσταση νέων υπολογιστικών συστημάτων αλλά και κατά την λειτουργία τους. Έτσι αφήνουν τα συστήματα τους ευπαθή σε διάφορους τύπους επιθέσεων.

Στη συνέχεια παραθέτονται κάποια στατιστικά στοιχεία από κρούσματα παραβίασης που καταγράφτηκαν στη Αμερική από την « info security analysis » την περίοδο 2000-2007. Η παρουσίαση περιλαμβάνει μια γενική στατιστική αναφορά σε παραβιάσεις δεδομένων ανά τύπου οργανισμών (εταιρικοί , εκπαιδευτικοί , υγείας και κρατικοί) με μετρήσεις που έγιναν από το 2000 μέχρι και το 2007 σε όλες τις πολιτείες των Ηνωμένων Πολιτειών. Επίσης περιλαμβάνει και μια πιο λεπτομερή ένδειξη για διάφορους τύπους παραβιάσεων ασφαλείας και παραθέτει με βάση αυτά τα ποσοστά των καταγραφών , των συμβάντων (records) καθώς και την πηγή προέλευσή αυτών. [4]

Συμβάντα και δεδομένα Παραβιάσεων ανά οργανισμούς

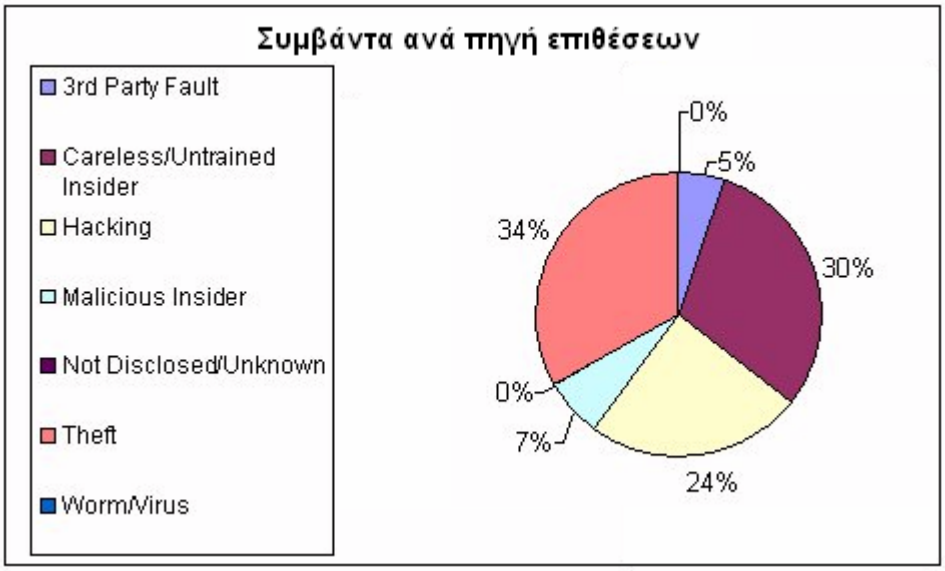


Συμβάντα και δεδομένα ανά παραβιάσεις

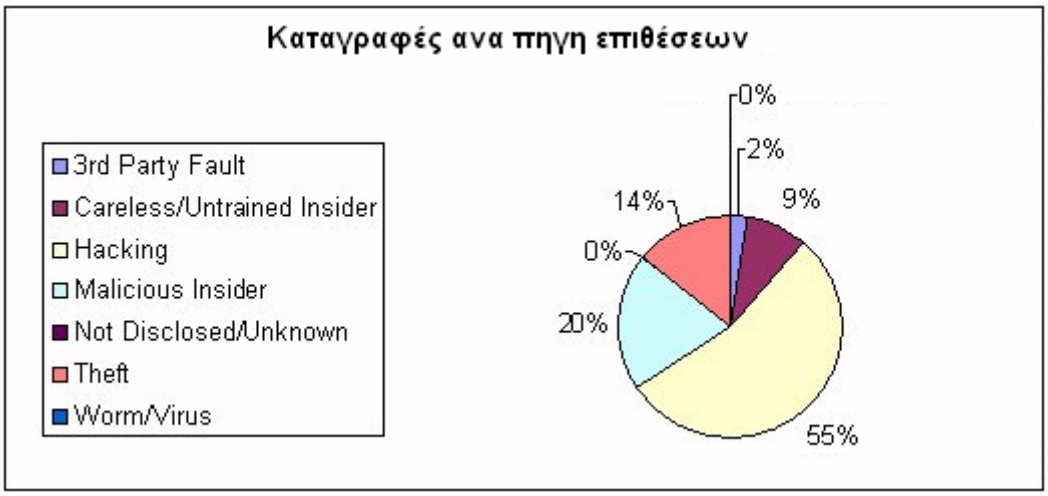


Τύποι Παραβιάσεων	**Καταγραφές**
Unknown	1081187
Data Breach	238089986
Data Exposure	17530796
Laptop	32100179
Media Loss	176935

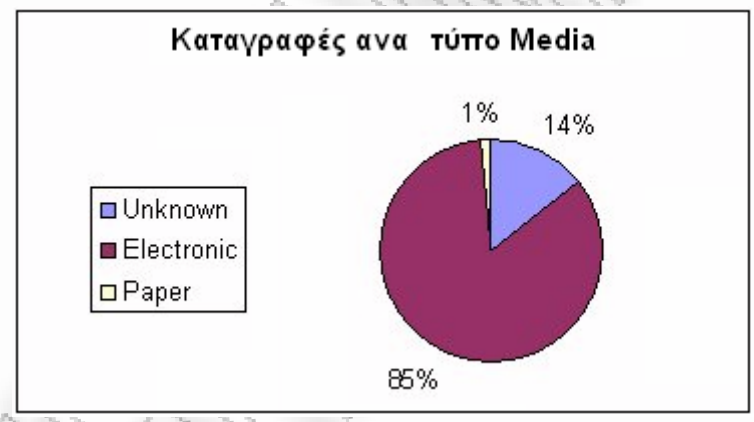
Τύποι Παραβιάσεων	Συμβάντα
Unknown	16
Data Breach	431
Data Exposure	248
Laptop	171
Media Loss	73



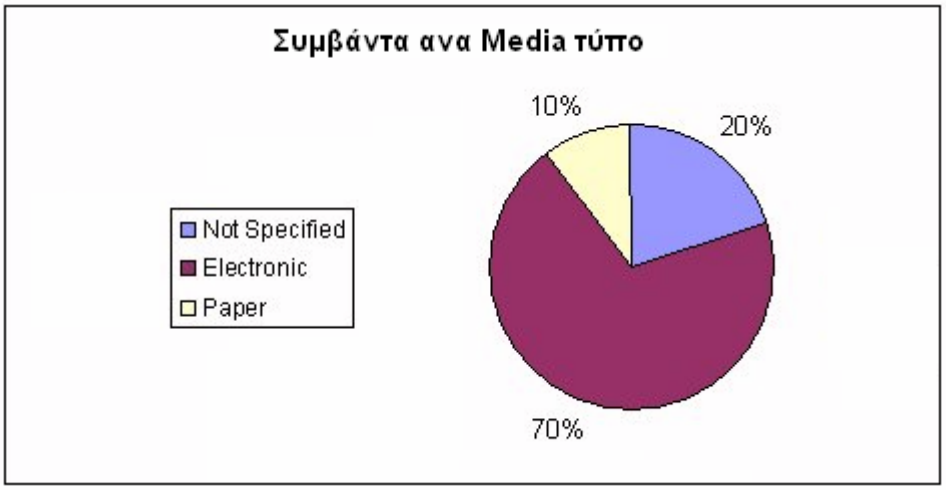
Πηγή Παραβιάσεων	Συμβάντα
3rd Party Fault	51
Careless/Untrained Insider	284
Hacking	225
Malicious Insider	65
Not Disclosed/Unknown	9
Theft	312
Worm/Virus	1



Πηγή Παραβιάσεων	**Καταγραφές**
3rd Party Fault	7460138
Careless/Untrained-Insider	28215809
Hacking	165631815
Malicious Insider	61732008
Not Disclosed/Unknown	112800
Theft	43145611
Worm/Virus	197518



Media	**Καταγραφές**
Unknown	44381579
Electronic	258203715
Paper	3910405



Media	**Συμβάντα**
Unknown	135
Electronic	523
Paper	53

Σημείωση: Τα νούμερα από τις δύο παραπάνω καταγραφές δεν είναι παρά μόνο ένα μεγάλο δείγμα των συνολικών κρουσμάτων και θα πρέπει να χρησιμοποιούνται σαν αναφορές και όχι σαν απόλυτα νούμερα.

1.3 Οικονομικές απώλειες από προβλήματα ασφαλείας

Οι οικονομικές απώλειες , που οφείλονται σε προβλήματα ασφαλείας πληροφοριακών συστημάτων και αναφέρθηκαν παραπάνω , είναι πολύ μεγάλες και έχουν αυξητικό χαρακτήρα κατά τα τελευταία χρόνια. Αυτές οι απώλειες οφείλονται κυρίως σε απάτη με σκοπό το κέρδος, σε κακόβουλες πράξεις που αποσκοπούν την ζημίωση ή και σε γεγονότα όπως για παράδειγμα η καταστροφή δεδομένων από ιούς.

Το μεγαλύτερο μέρος των επιθέσεων προέρχεται κυρίως από το Internet και από το εσωτερικό της επιχείρησης αλλά και από πρώην εργαζόμενους της. Το μεγαλύτερο μέρος των ερωτηθέντων (73%) αναφέρει το Internet σαν συχνό σημείο επίθεσης παρά τα εσωτερικά τους συστήματα (36%).

Ειδικοί αναλυτές για θέματα ασφαλείας υπολογίζουν τις απώλειες σε παγκόσμιο επίπεδο σε πολλά δισεκατομμύρια δολάρια ετησίως. Το μέγεθος των απωλειών μπορεί να είναι αρκετά μεγάλο ώστε να καταστρέψει ολόκληρες εταιρίες και οργανισμούς ή να θέσει εκτός ανταγωνισμού όσους αρνούνται να δουν τα θέματα ασφαλείας των υπολογιστικών συστημάτων ως σημαντικό ρίσκο της λειτουργίας ενός οργανισμού.

Συνεπώς επενδύοντας σωστά στο τομέα της ασφάλειας υπάρχει μείωση του ρίσκου για τυχών περιστατικά υποκλοπής , καταστροφής η κακόβουλης αλλαγής της περιουσίας κάθε οργανισμού. Βέβαια σε αυτό το σημείο αξίζει να αναφερθεί πως η κακή χρήση των μέτρων ασφαλείας μπορεί να αποβεί και ως οικονομική απώλεια σε περιπτώσεις που καθιστά δύσκολο το έργο τον εργαζομένων και υπάρχει μείωση στην αποδοτικότητά τους. Για αυτό το λόγο η μελέτη της ασφάλειας σε ένα σύστημα πρέπει να γίνει από ειδικούς και με μεγάλη προσοχή , προσαρμόζοντάς την διαφορετικά σε κάθε περίπτωση και εκεί που είναι απαραίτητη. [3]

1.4 Αντιμετώπιση – Δράση και όχι Αντίδραση

Όπως αναφέρθηκε και παραπάνω η αντιμετώπιση της ασφάλειας σε κάθε οργανισμό πρέπει να γίνεται προσεχτικά και πάνω από όλα , από ειδικούς. Είναι σύνηθες το φαινόμενο, κυρίως στις μικρότερους οργανισμούς αλλά και από μεγάλους , να δίνουν έμφαση στην ασφάλεια μετά το πρώτο πλήγμα – απώλεια, και αυτό το κάνουν ως αντίδραση και όχι σαν πρόνοια. Η αντιμετώπιση της ασφάλειας θα πρέπει να περάσει από τη λογική της αντίδρασης, σε εκείνη της δράσης μέσα από τον εκ των προτέρων καθορισμό απαιτήσεων. Το κριτήριο που θα πρέπει να καθοδηγεί τις απαιτήσεις ασφαλείας είναι το «μην γίνεται τίποτα, εκτός αν είναι απολύτως απαραίτητο». Επιπρόσθετα, οι απαιτήσεις θα πρέπει να είναι ξεκάθαρες και εύληπτες από όλους τους εμπλεκόμενους ενώ ουσιαστική και κρίσιμη θα πρέπει να είναι η συμμετοχή της ανώτατης διοίκησης. Η ασφάλεια είναι κάτι που είναι υπερβολικά σημαντικό για να αποτελεί αποκλειστική ευθύνη των τεχνικών. Αρκεί η αναφορά για τις οικονομικές απώλειες -ή και τη χρεοκοπία- που έπονται ενός σοβαρού περιστατικού ασφαλείας.

“Στον ιστό της ζωής, τα πάντα συνδέονται μεταξύ τους” λέει ένα ρητό των ινδιάνων. Η διατύπωση αυτή αποδεικνύεται επίκαιρη και σχετική στον τομέα της ασφάλειας της Πληροφορικής. Κοινό πρόβλημα αποτελεί ο κατακερματισμός της ασφάλειας και η έλλειψη μιας συνολικής θεώρησης. Η σημαντικότερη ιδέα είναι η απόλυτη ανάγκη για μια ολιστική προσέγγιση της ασφάλειας. Βασική προϋπόθεση είναι να ξεκινά κανείς με ένα γενικό σχεδιασμό της υποδομής ασφάλειας που επιθυμεί να δημιουργήσει και όχι να κάνει αποσπασματικές κινήσεις και τα μπαλώματα που αυτές επιτάσσουν στη συνέχεια. Η δεύτερη αυτή προσέγγιση στοιχίζει άλλωστε συνήθως 10 φορές περισσότερο απ’ ότι η πρώτη. Παράλληλα, η ασφάλεια δεν θα πρέπει να αντιμετωπίζεται σαν Project αλλά σαν πεδίο που μένει πάντα «ανοικτό» και όπου απαιτείται διαρκής εξέλιξη.

Άλλη μια αλληγορία για να φανεί ο βαθμός ασφάλειας που πρέπει να υπάρχει σε έναν οργανισμό είναι το “Jailer’s paradox” , το Παράδοξο του Φυλακισμένου, βάσει του οποίου η ζωή ενός φύλακα είναι πολύ δυσκολότερη από εκείνη ενός φυλακισμένου. Ενώ ο φυλακισμένος ψάχνει να βρει μία και μόνο δίοδο για να δραπετεύσει, έχοντας στη διάθεσή του όλο το χρόνο, ο φύλακας προσπαθεί να προβλέψει όλους τους πιθανούς τρόπους απόδρασης, με περιορισμούς από χρονικής άποψης.

Αντίστοιχα, η δραστηριότητα του οργανωμένου εγκλήματος είναι συχνά πολύ πιο εξελιγμένου επιπέδου απ’ ότι εκείνη των υπεύθυνων για την ασφάλεια Πληροφορικής. Εννοείται δε ότι ο χρόνος, οι πόροι και τα κίνητρα που έχουν στη διάθεσή τους οι πρώτοι δεν συγκρίνονται με τα αντίστοιχα των δεύτερων. [11]

Η αντιμετώπιση των προβλημάτων ασφαλείας, παρότι δεν είναι απλή υπόθεση, πρέπει να λαμβάνεται σοβαρά υπόψη. Η εισαγωγή πληροφοριακών συστημάτων σε ένα περιβάλλον μπορεί μεν να αυξάνει κατακόρυφα την παραγωγικότητα και το κέρδος, αλλά εισάγει νέους κινδύνους που αυξάνουν σημαντικά το ρίσκο και επομένως πρέπει οπωσδήποτε να αναγνωριστούν και να αντιμετωπιστούν ανάλογα. Ο κλάδος της ασφάλειας πληροφοριακών συστημάτων έχει να προσφέρει ευτυχώς μια πληθώρα από αντίμετρα (εργαλεία, μεθόδους, έλεγχους, πολιτικές ασφαλείας) για την αντιμετώπιση κάθε είδους προβλήματος. Η ενσωμάτωση όμως όλων αυτών σε κάθε οργανισμό δεν είναι καθόλου απλή υπόθεση. Αντιθέτως, ο διαφορετικός τρόπος λειτουργίας καθώς και η διαφορετική ανάθεση πόρων για θέματα ασφαλείας δημιουργούν εντελώς διαφορετικές συνθήκες, μοναδικές για κάθε οργανισμό.

Η ενσωμάτωση της ασφάλειας λοιπόν δεν πρέπει να θεωρηθεί ως μια απλή διαδικασία, καθώς πρέπει κάθε φορά να λαμβάνονται υπόψη όλοι οι παράγοντες, έτσι ώστε η ασφάλεια να μην γίνετε εμπόδιο στην λειτουργία του οργανισμού αλλά να τον υπηρετεί.

Λύση στο πρόβλημα αυτό δίνει η ανάλυση κινδύνων (risk analysis). Η ανάλυση κινδύνων έχει ως σκοπό την αξιολόγηση των περιουσιακών στοιχείων του οργανισμού και την αναγνώριση όλων των κινδύνων και των ευπαθειών που τα απειλούν. Θα πρέπει στο σημείο αυτό να αναφερθεί ότι με τον όρο «περιουσιακά στοιχεία» δεν εννοούνται μόνο τα καθαρά οικονομικά μεγέθη. Αντιθέτως, συμπεριλαμβάνονται και αξίες όπως προσωπικά δεδομένα, στοιχεία που η παραβίαση τους μπορεί να οδηγήσει στην απώλεια ανθρώπινης ζωής, η εικόνα ενός οργανισμού προς τα έξω κτλ. Με τα δεδομένα αυτά υπολογίζεται το ρίσκο που εισάγει η χρήση κάθε πληροφοριακού συστήματος στην λειτουργία του οργανισμού. Έτσι, μπορούν να υπολογιστούν με ικανοποιητική ακρίβεια ποια αντίμετρα συμφέρει να εγκατασταθούν και σε ποιες περιπτώσεις είναι προτιμότερη η αποδοχή του ρίσκου. Επιπρόσθετα, η ανάλυση κινδύνων θέτει προτεραιότητες στα αντίμετρα που μπορούν να εγκατασταθούν, με αποτέλεσμα να μπορεί να γίνει μια πιο ορθή επιλογή στις περιπτώσεις που ο προϋπολογισμός δεν επιτρέπει αρκετούς πόρους ώστε να καλυφθούν όλες οι ανάγκες για θέματα ασφαλείας. Ιδιαίτερα σήμερα που η παγκόσμια οικονομία βρίσκεται σε ύφεση και οι περισσότερες επιχειρήσεις και οργανισμοί αναγκάζονται να κάνουν περικοπές σε όλους τους τομείς, η ανάλυση κινδύνων έρχεται να παίξει ουσιαστικό ρόλο στην σωστή αντιμετώπιση των προβλημάτων ασφαλείας με οργανωμένο και αποτελεσματικό τρόπο.

1.5 **Σχεδιασμός για το απροσδόκητο** (Planning for the Unexpected)

Η διαχείριση της επιχειρησιακής συνέχειας Business continuity management (BCM) ασχολείται με τη διαχείριση του κινδύνου για να εξασφαλίσει ότι, ανά πάσα στιγμή, ένας οργανισμός μπορεί να συνεχίσει να λειτουργεί, τουλάχιστον, σε ένα προκαθορισμένο ελάχιστο επίπεδο. Αυτή θα πρέπει να επικεντρωθεί σε όλες τις επιχειρηματικές διαδικασίες και όχι μόνο σε συγκεκριμένα «περιουσιακά» στοιχεία, όπως τα συστήματα του IT.

Η αποτελεσματική συνέχιση της επιχειρηματικής δραστηριότητας αποτελεί ουσιώδες μέρος της δυνατότητας για τη διαχείριση του κάθε οργανισμού. Όποια και αν είναι η επιχειρηματική κατεύθυνση ενός οργανισμού, ο βασικός στόχος πρέπει να παραμένει ίδιος. Αυτός είναι η παροχή μιας συνεπής και αποδεκτής μεθοδολογίας για την εξασφάλιση μίας συγκεκριμένης και υποστηριζόμενης προσέγγισης για την εφαρμογή της διαχείρισης της επιχειρησιακής συνέχειας. Η προσέγγιση δίνει έμφαση όχι μόνο για τη δυνατότητα της ανάκτησης των βασικών στοιχείων των λειτουργιών του κάθε οργανισμού αλλά και για την διατήρηση της υπάρχων φήμης, για την εξασφάλιση ενός σταθερού εισοδήματος ροής ,τη συμμόρφωση με τις καταστατικές υποχρεώσεις , στον εντοπισμό των σημαντικών επιπτώσεων και κινδύνων και τέλος στην επικέντρωση για την ελαχιστοποίηση των κινδύνων που εμφανίζονται. [5]

1.6 Συνοχή Πληροφοριακού Συστήματος

Η μεθοδολογία για την επίτευξη της συνοχής των πληροφοριακών συστημάτων είναι χτισμένη γύρω από έξι βασικές αρχές: Προστασία, Αναγνώριση-Εντοπισμός, Αντίδραση, Ανάκτηση, Συνέχιση και Επιστροφή.

Προστασία
Η προστασία του περιβάλλοντος ενός πληροφοριακού συστήματος είναι ζωτικής σημασίας για τη διατήρηση των επιθυμητών επιπέδων της διαθεσιμότητας για έναν οργανισμό. Οι υπηρεσίες του Π.Σ. απειλούνται από περιβαλλοντικές αποτυχίες (environmental failures), σφάλματα υλικού (hardware failures), λειτουργικά σφάλματα (operational errors) και κακόβουλες επιθέσεις (malicious attack).

Αναγνώριση-Εντοπισμός
Με την ανίχνευση συμβάντων ελαχιστοποιούνται οι επιπτώσεις στις υπηρεσίες, μειώνεται η προσπάθεια ανάκτησης, και διατηρείται η ποιότητα των παρεχόμενων υπηρεσιών.

Αντίδραση
Η αντίδραση σε ένα περιστατικό με τον καταλληλότερο τρόπο, θα επιτρέψει την αποτελεσματική ανάκτηση και αν υπάρξει χρόνος εκτός λειτουργίας το λεγόμενο downtime, θα μείνει στο ελάχιστο. Από την αντίθετη πλευρά αν υπάρχει κακή αντίδραση σε κάποιο συμβάν τότε μπορεί ένα ασήμαντο περιστατικό να κλιμακωθεί σε κάτι πολύ πιο σοβαρό.

Ανάκτηση
Η ανάκτηση των υπηρεσιών πρέπει να γίνεται με ένα ελεγχόμενο και προκαθορισμένο τρόπο. Προσδιορίζοντας και εφαρμόζοντας το κατάλληλο στρατηγικό πλάνο αποκατάστασης διασφαλίζεται η έγκαιρη αποκατάσταση των υπηρεσιών και η διατήρηση της ποιότητας των δεδομένων.

Συνοχή
κατανόηση των προτεραιοτήτων ανάκαμψης, καθώς το σημείο ανάκαμψης και ο χρόνος αποκατάστασης επιτρέπει την ιεραρχική αποκατάσταση των υπηρεσιών (διαχωρισμός κρίσιμων και μη υπηρεσιών . Υπηρεσίες που είναι λιγότερο κρίσιμες αποκαθίσταντο σε μεταγενέστερο χρόνο ενώ οι κρίσιμες σε πρώτο χρόνο.

Επιστροφή
Η διαδικασία της επιστροφής, από κατάσταση καταστροφής στην κανονική λειτουργία, είναι συχνά παραμελημένη από τους οργανισμούς. Όλος ο μηχανογραφικός σχεδιασμός θα πρέπει να έχει μια στρατηγική εξόδου, η οποία να επιτρέπει σε οποιαδήποτε στιγμή την ανάκτηση του μηχανογραφικό κέντρου από καταστροφή.

Παρακάτω παραθέτονται τα έξι βασικά στοιχεία που βοηθούν την πρόοδο ενός οργανισμού μέσω αυτού του ώριμου μοντέλου IT continuity. [5,6]

- Συνεχείς ανασκοπήσεις, εντατικές καταγραφές και ελέγχους υγείας
- Προσδιορισμός ανθεκτικότητας και στρατηγικές αποκατάστασης
- Σχεδιασμός και η υλοποίηση λύσεων
- Πλάνο αποκατάστασης καταστροφών
- Πλάνο συνοχής και δοκιμές ανάκτησης

• Συνεχή κατάρτιση των υπεύθυνων του τμήματος IT.

2 Ανάλυση Κινδύνων (Risk Analysis)

2.1 Εισαγωγή

Ξεκινώντας με την ανάλυση των κινδύνων είναι σημαντικό να μελετηθεί η τοπολογία των συστημάτων. Στο παρελθόν σε έναν οργανισμό το πληροφοριακό σύστημα βρισκόταν συγκεντρωμένο κεντρικά σε ένα σημείο λόγω τις χρήσης mainframe συστημάτων. Η ασφάλεια του ήταν πολύ πιο απλή πιο προσιτή και παράλληλα πιο εύκολα εφαρμόσιμη. Σήμερα όμως το περιβάλλον των πληροφοριακών συστημάτων συνήθως είναι αρκετά διαφορετικό. Δεδομένα και πληροφορίες είναι διασκορπισμένες σε τοπικά δίκτυα και διαφορετικά συστήματα τμημάτων, ώστε να αντικαταστήσουν την συγκεντρωμένη λογική των mainframe. Τα κατανεμημένα συστήματα και η πολυπλοκότητα των δικτύων συντάσσουν πολύ πιο πολυσύνθετες συνθήκες διαχείρισης και ασφάλειας.

Για να μπορέσει να υπολογιστεί ικανοποιητικά η πιθανότητα να συμβεί ένα ανεπιθύμητο γεγονός και το μέγεθος του, πρέπει να υπάρχει μια γνώση των στοιχείων που απαρτίζουν τον κίνδυνο καθώς και των συσχετίσεων μεταξύ τους. Με καλή γνώση του κινδύνου μπορεί κάποιος να αποφασίσει ευκολότερα και σωστότερα για το αν θα αποδεχτεί τον κίνδυνο έτσι όπως έχει αποτιμηθεί ή αν θα προβεί σε ενέργειες που θα τον αποτρέψουν ή θα τον μειώσουν σε αποδεκτά επίπεδα. Αυτός με λίγα λόγια είναι ο σκοπός της ανάλυσης κινδύνων (risk analysis).

2.2 Ορισμοί

Για καλύτερη κατανόηση παρουσιάζονται παρακάτω οι βασικοί ορισμοί που χρησιμοποιούνται στην ανάλυση κινδύνων:

Απειλή: Ένα μη επιθυμητό γεγονός που μπορεί να προκαλέσει μη διαθεσιμότητα του συστήματος και των υπηρεσιών, τυχαία ή με πρόθεση μμετατροπή των δεδομένων, καταστροφή των δεδομένων ή του συστήματος και τέλος μη εξουσιοδοτημένη αποκάλυψη ευαίσθητων πληροφοριών.

Ευπάθεια: Μια αδυναμία ή σχεδιαστική ατέλεια σε ένα σύστημα, εφαρμογή ή υποδομή που μπορεί να γίνει αιτία για την παραβίαση της ασφάλειας και της ακεραιότητας του συστήματος.

Κίνδυνος: Η πιθανότητα μια συγκεκριμένη απειλή να εκμεταλλευτεί μια συγκεκριμένη ευπάθεια. Εναλλακτικά ο κίνδυνος, ο οποίος εκφράζει το ενδεχόμενο για απώλεια, μπορεί να εκφραστεί καλύτερα με την απάντηση των παρακάτω ερωτήσεων:

1. Τι θα μπορούσε να συμβεί; (Απειλή)
2. Πόσο κακό θα μπορούσε να είναι; (Συνέπειες)
3. Πόσο συχνά μπορεί να συμβαίνει; (Συχνότητα)
4. Τι σιγουριά υπάρχει για τις απαντήσεις στις 3 παραπάνω ερωτήσεις; (Βαθμός αβεβαιότητας)

Αντίμετρο: Μέτρο που λαμβάνεται για την προστασία του πληροφοριακού συστήματος και την αντιμετώπιση των απειλών. Το μέτρο μπορεί να ενεργεί ανιχνεύοντας, προλαμβάνοντας ή μειώνοντας την απώλεια που σχετίζεται με την εμφάνιση μιας απειλής ή κατηγορίας απειλών.

Ανάλυση κινδύνων: Ανάλυση κινδύνων ενός πληροφοριακού συστήματος είναι η διαδικασία αναγνώρισης και αξιολόγησης των κινδύνων ασφαλείας που εισάγει το σύστημα στην λειτουργία ενός οργανισμού, καθώς και το κόστος των απωλειών που θα προκληθούν σε περίπτωση που δημιουργηθεί πρόβλημα ασφαλείας. Έτσι προσδιορίζεται ο βαθμός κινδύνου του πληροφοριακού συστήματος και οι απαιτήσεις ασφαλείας που υπάρχουν. Υπολογίζεται επιπλέον και το κόστος πρόληψης κάθε απώλειας ώστε να είναι δυνατή μια σωστή αντιμετώπιση των κινδύνων με ορθολογιστικά κριτήρια.

2.3 Υπολογισμός Ανάλυσης Κινδύνων

Η καρδιά της ανάλυσης κινδύνων ορίζεται από τον εξής τύπο

$$B > P * L$$

όπου ,
B ορίζεται το κόστος για την πρόληψη μίας απώλειας,
P η πιθανότητα να συμβεί μια απώλεια και
L το συνολικό κόστος μιας απώλειας.

Το νόημα αυτού του βασικού τύπου είναι πως στην περίπτωση που το κόστος της πρόληψης μιας απώλειας (B) είναι μεγαλύτερο από το γινόμενο του κόστους της απώλειας επί την πιθανότητα να συμβεί αυτή (P * L) τότε η υλοποίηση του μέτρο πρόληψης κρίνεται ως υπερβολική. Σε αντίθετη περίπτωση το μέτρο πρόληψης συμφέρει να υλοποιηθεί.

Συνήθως τα μεγέθη αυτά υπολογίζονται σε ετήσιες απώλειες και ετήσια πιθανότητα να συμβεί ένα γεγονός. Ο τύπος αυτός αντικατοπτρίζει ουσιαστικά την κεντρική ιδέα πίσω από κάθε ανάλυση κινδύνων και όχι μόνο για πληροφοριακά συστήματα. Είναι η ιδέα του υπολογισμού της πιο συμφέρουσας λύσης.

Βέβαια, παρόλη την απλοϊκότητα που δείχνει ο τύπος BPL , ο υπολογισμός αυτού καθώς και η πρακτική του εφαρμογή βρίσκει σημαντικές δυσκολίες. Ο ακριβής υπολογισμός των τιμών των πιθανοτήτων, του κόστους πρόληψης και της απώλειας δεν είναι πάντα εύκολος ή δυνατός. Ένα απλό παράδειγμα είναι η αντιστοίχηση των απωλειών με τα οικονομικά νούμερα. Σε αυτές τις περιπτώσεις η ζητούμενη αντιστοίχηση δεν είναι πάντα εφικτή για το λόγο ότι πολλές φορές στην ανάλυση κινδύνων αξιολογούνται απώλειες απροσδιόριστες όπως η εικόνα ενός οργανισμού και η εμπιστοσύνη που έχουν οι «πελάτες» του σε αυτόν. Παρόλο που δεν χρησιμοποιείται άμεσα, όλες οι μέθοδοι της ανάλυσης κινδύνων βασίζονται πάνω στην κεντρική λογική του τύπου BPL. [3]

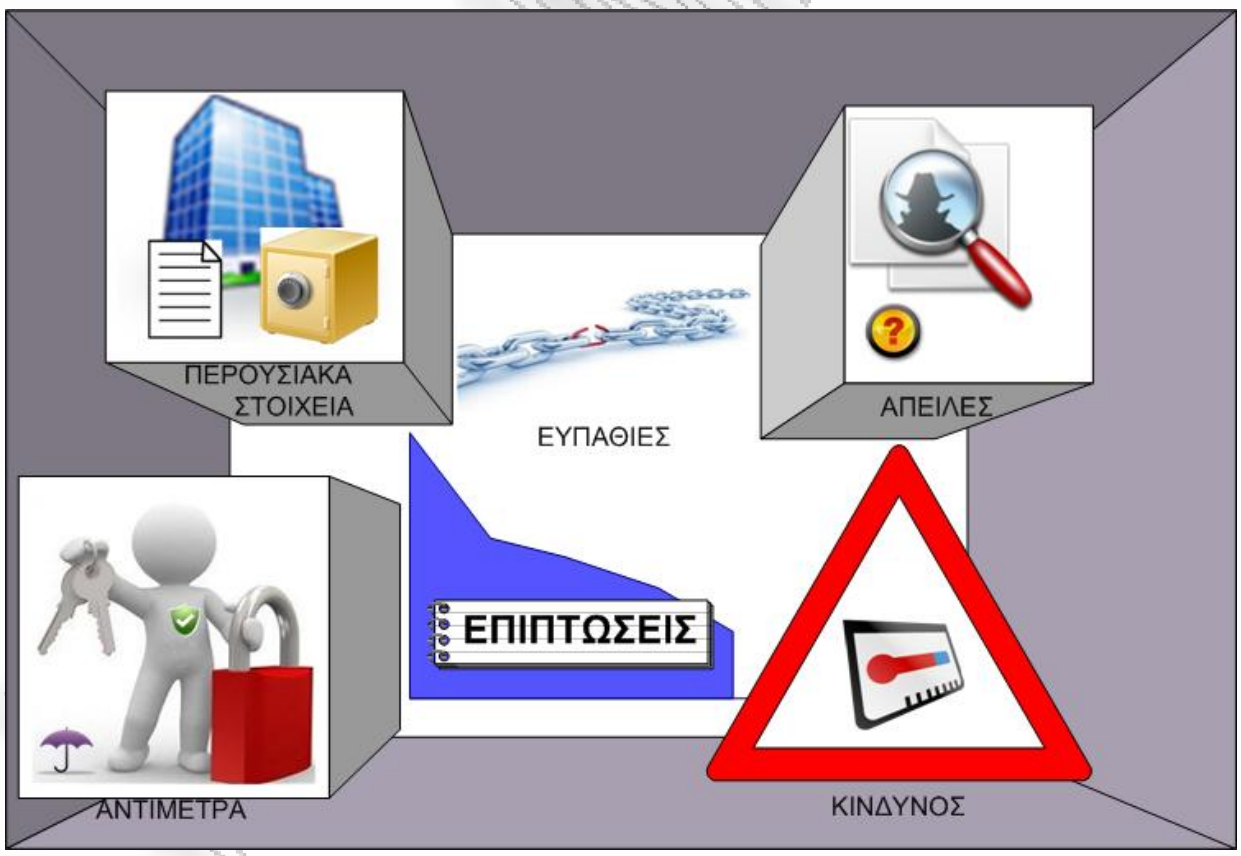
2.4 Βασική μεθοδολογία της ανάλυσης κινδύνων

Προκειμένου οι διαχειριστές να πάρουν σωστές αποφάσεις για την αποδοχή, αποτροπή ή μείωση των κινδύνων και την υλοποίηση αποδοτικών οικονομικά (cost effective) λύσεων ασφαλείας, είναι αναγκαία η υιοθέτηση μιας μεθοδολογίας που θα αντιμετωπίζει τα θέματα με βάση το κόστος και το όφελος. Με τον καιρό έχει δημιουργηθεί μια πληθώρα διαδικασιών που ήρθαν να καλύψουν διαφορετικές ανάγκες για ανάλυση κινδύνων. Αν και υπάρχουν πολλές διαφορετικές διαδικασίες, η βασική μέθοδος παραμένει η ίδια.

Ο κίνδυνος στον οποίο εκτίθεται ένα πληροφοριακό σύστημα είναι συνάρτηση:

- Της αξίας των περιουσιακών στοιχείων
- Των ευπαθειών του
- Των πιθανών απειλών και της φύσης τους
- Των επιπτώσεων που μπορεί να προκύψουν

Στο παρακάτω σχήμα φαίνονται οι σχέσεις μεταξύ των παραπάνω καθώς και η σχέση του κινδύνου με τα αντίμετρα που τελικά επιλέγονται.



Τα περιουσιακά στοιχεία έχουν κάποιες ευπάθειες, τις οποίες εκμεταλλεύονται οι διάφορες

απειλές με συνέπεια τις ανάλογες επιπτώσεις. Όλα αυτά υπολογίζονται και συνεπάγουν τα αντίμετρα με σκοπό να μειώσουν τους κινδύνους που υπάρχουν. [3]

Η βασική μεθοδολογία της ανάλυσης κινδύνων αποτελείται από τις παρακάτω διαδικασίες:

1. Καθορισμός σκοπών και εμβέλειας της ανάλυσης

   Η διαδικασία αυτή καθορίζει τι ακριβώς θα περιληφθεί στην ανάλυση κινδύνων και ποια τα πιθανά αποτελέσματα αναμένονται να παραχθούν από αυτήν.

2. Αναγνώριση και αξιολόγηση περιουσιακών στοιχείων του πληροφοριακού συστήματος

   Επειδή πολλά από τα περιουσιακά στοιχεία ενός οργανισμού δεν είναι εύκολα αναγνωρίσιμα, υπάρχει διαδικασία εντοπισμού τους και προσδιορισμός της αξίας τους προς τον οργανισμό.

3. Ανάλυση απειλών ανά περιουσιακά στοιχεία και μελέτη επιπτώσεων που πιθανόν να εμφανίσουν:

   Κάθε κατηγορία περιουσιακών στοιχείων παρουσιάζει και μια σειρά απειλών. Η διαδικασία αυτή ξεκινάει με την αναγνώριση αυτών για κάθε περιουσιακό στοιχείο, και επέρχεται η μελέτη του τρόπου με τον οποίο απειλείται, και οι επιπτώσεις που θα επιφέρει η κάθε απειλή.

4. Ανάλυση ευπαθειών:

   Η διαδικασία αυτή γίνεται για να διευκρινίσει την ευπάθεια του κάθε περιουσιακού στοιχείου προς κάθε απειλή ξεχωριστά. Ένα περιουσιακό στοιχείο δηλαδή μπορεί να είναι λιγότερο ευπαθής προς μια απειλή και περισσότερο σε μια άλλη.
   Η ευπάθεια μπορεί να οριστεί και με την εξής συνάρτηση:

   Ευπάθεια = Πιθανότητα να συμβεί μια απειλή $\boldsymbol{x}$ *Πιθανότητα να είναι επιτυχής*

5. Υπολογισμός κινδύνου:

   Ο υπολογισμός του κινδύνου γίνεται ξεχωριστά για κάθε απειλή προς κάθε περιουσιακό στοιχείο, όπως αναφέρθηκε και παραπάνω, και βαθμολογείται . Ο βαθμός του κινδύνου είναι μια συνάρτηση όλων των παραπάνω, δηλαδή, των επιπτώσεων μιας απειλής (που έχουν σχέση με την αξία του περιουσιακού στοιχείου) και της ευπάθειας του περιουσιακού στοιχείου ως προς αυτή.

6. Επιλογή τρόπων αντιμετώπισης των κινδύνων:

Οι τρόποι αντιμετώπισης του κινδύνου είναι τρεις:
α) **Αποφυγή** του κινδύνου με πλήρη απόσυρση από μια συγκεκριμένη
β) **Αποδοχή** του κινδύνου
γ) **Μείωση** του κινδύνου με χρήση αντιμέτρων (μέτρων ασφαλείας)

Η αποφυγή του κινδύνου δηλώνει την πλήρη απόσυρση από τη συγκεκριμένη απειλή, η αποδοχή σηματοδοτεί μια απάθεια προς τον κίνδυνο και η μείωση εκφράζει τη χρήση μέτρων ασφαλείας – τα λεγόμενα αντίμετρα. Με τα αντίμετρα μπορούν να επιτευχθούν τα εξής:

- Μεταφορά κινδύνου
  πχ. αγορά ασφάλειας

- Μείωση ευπάθειας:

  - Μείωση πιθανότητας να συμβεί μια απειλή
    περιορισμός σε ευαίσθητες περιοχές (πχ κάπνισμα)
  - Μείωση πιθανότητας μια απειλή να είναι επιτυχής
    χρήση κρυπτογράφησης, χρήση firewall

- Μείωση αντίκτυπου
  πχ. σύστημα πυρόσβεσης

- Μέτρα ανάνηψης (επαναφοράς)
  πχ. backup

Με αυτή τη διαδικασία αναγνωρίζονται τα πιθανά αντίμετρα που μπορούν να εφαρμοστούν και επιλέγονται αυτά που συμφέρουν περισσότερο τον οργανισμό.

Όπως έχει αναφερθεί και στην αρχή του κεφαλαίου η ανάλυση κινδύνων και η ασφάλεια των πληροφοριακών συστημάτων γενικότερα είναι μια συνεχόμενη διαδικασία. Μετά την επιλογή των τρόπων αντιμετώπισης και την εφαρμογή τους στον οργανισμό, πρέπει να υπάρχει μια συνεχής παρακολούθηση των κινδύνων. Τα δεδομένα και οι λειτουργίες σε ένα πληροφοριακό σύστημα είναι λογικό και επόμενο να αλλάζουν συνεχώς, με νέες απειλές, νέες ευπάθειες, νέες επιπτώσεις κτλ. Τα αντίμετρα λοιπόν που έχουν επιλεχθεί πρέπει ελέγχονται συνεχώς για την αποτελεσματικότητα τους και όχι να μένουν στάσιμα. Πολλά από αυτά με τον καιρό σταματούν να συμφέρουν τον οργανισμό με συνέπεια είτε την κατάργησή τους είτε την αντικατάστασή τους από νέα. [3]

2.5 Οφέλη της ανάλυσης κινδύνων

Παρακάτω αναφέρονται τα πιο σημαντικά οφέλη που αποκομίζονται από την ανάλυση κινδύνων πληροφοριακών συστημάτων.

Γενική βελτίωση της ασφάλειας του πληροφοριακού συστήματος

Η ανάλυση κινδύνων βοηθάει στην γενική βελτίωση της ασφάλειας του πληροφοριακού συστήματος αναγνωρίζοντας και αντιμετωπίζοντας τους σημαντικότερους κινδύνους που το απειλούν.

Στόχευση της ασφάλειας

Η ασφάλεια πρέπει να στοχεύει κατάλληλα και άμεσα στις πιθανές επιπτώσεις, απειλές και υπάρχουσες ευπάθειες. Η αποτυχία να γίνει αυτό μπορεί να οδηγήσει σε υπερβολικές και μη αναγκαίες δαπάνες. Η ανάλυση κινδύνων προάγει πολύ καλύτερη στόχευση που βοηθά στην εξάλειψη των άσκοπων δαπανών και στην πιο αποτελεσματική αντιμετώπιση των πραγματικών προβλημάτων ασφαλείας.

Βελτίωση της κατανόησης του συστήματος

Κατά την διαδικασία της ανάλυσης κινδύνων βελτιώνεται η γνώση και η κατανόηση του συστήματος ως προς θέματα ασφαλείας. Καταρχάς αναγνωρίζονται οι διάφορες απειλές και φανερώνονται οι ευπάθειες του. Επίσης κατανοείται η πραγματική αξία των επιμέρους συστημάτων που αποτελούν το πληροφοριακό σύστημα.

Κατανόηση της αναγκαιότητας της ασφάλειας

Η συμμετοχή στην διαδικασία της ανάλυσης κινδύνων διαμορφώνει μια καλύτερη κατανόηση των προβλημάτων ασφαλείας καθώς και των επιπτώσεων που μπορεί να έχουν αυτά. Με αυτό τον τρόπο επιτυγχάνεται καλύτερη επιλογή αντιμέτρων αλλά και μεγαλύτερη αποδοχή των αντιμέτρων που προτείνονται από τους χρήστες. Η κατανόηση της αναγκαιότητας της ασφάλειας έχει ως αποτέλεσμα την αντιμετώπιση των θεμάτων ασφαλείας με την σοβαρότητα που τους αρμόζει.

Δικαιολόγηση δαπανών για την ασφάλεια

Η εισαγωγή ασφάλειας σε ένα πληροφοριακό σύστημα σχεδόν πάντα σημαίνει επιπλέον κόστος. Επειδή όμως δεν οδηγεί άμεσα σε αύξηση των κερδών μιας επιχείρησης, πρέπει να δικαιολογείται οικονομικά. Η ανάλυση κινδύνων δημιουργεί την κατάλληλη δικαιολόγηση για την αναγκαιότητα της ασφάλειας που προτείνεται και του κόστους που αυτή προσθέτει. [2]

ΠΡΑΚΤΙΚΟ ΜΕΡΟΣ

ΠΡΑΚΤΙΚΗ ΕΦΑΡΜΟΓΗ ΑΝΑΛΥΣΗΣ ΚΙΝΔΥΝΩΝ ΜΕ ΤΗΝ ΜΕΘΟΔΟ CRAMM

X MEDICALS CORPORATION

3.1.1 Εισαγωγή

Σε αυτό το μέρος θα γίνει η πρακτική εφαρμογή της ανάλυσης των κινδύνων στον οργανισμό X Medicals χρησιμοποιώντας τη μέθοδο και τα εργαλεία της CRAMM. Η εταιρία X Medicals είναι μία ιατρική εταιρία στην Ελληνική αγορά, στο χώρο του ιατρικού εξοπλισμού των χειρουργικών εργαλείων, των Ορθοπεδικών προϊόντων και των Νευροχειρουργικών εμφυτευμάτων υψηλής ποιότητας. Το εμπόριο ιατρικών ειδών και η τεχνική υποστήριξη είναι οι βασικές υπηρεσίες που παρέχει στα νοσοκομεία και τις κλινικές με σκοπό την παροχή υψηλής ποιότητας και τεχνολογίας προϊόντων και ουσιαστικά την βελτίωση της ποιοτικής ζωής βασισμένη σε μια φιλοσοφία με τις παρακάτω αρχές.

- Εξυπηρέτηση του πελάτη
- Συνεχής προσαρμογή – καινοτομία
- Ποιότητα σε προϊόντα και υπηρεσίες
- Θετική ατμόσφαιρα εργασίας

3.1.2 Σκοπός της ανάλυσης

Σκοπός της ανάλυσης κινδύνων στο πληροφοριακό σύστημα της εταιρίας που γίνεται η μελέτη είναι η αναγνώριση και αξιολόγηση των προβλημάτων ασφαλείας που υπάρχουν σε αυτό και επηρεάζουν την σωστή λειτουργία της. Με την ανάλυση κινδύνων θα μπορεί να εφαρμοστεί μια πιο οργανωμένη πολιτική αντιμετώπισης, ώστε να μειωθεί στο ελάχιστο το αντίκτυπο από τα προβλήματα αυτά.

3.1.3 Εμβέλεια της ανάλυσης

Η ανάλυση κινδύνων θα περιοριστεί στα κρίσιμα συστήματα και σε όλες τις βασικές υπηρεσίες του οργανισμού (mission critical), που είναι απαραίτητα για την σωστή λειτουργία του καθώς και σε backup ευαίσθητων δεδομένων που πρέπει να προστατευτούν. Στην ανάλυση δεν περιλαμβάνονται συστήματα που δεν έχουν άμεση επαφή τις βασικές υπηρεσίες που προσφέρει η εταιρία και τους βασικούς διακομιστές (servers) που τις υποστηρίζουν.

3.1.4 Μέθοδος και εργαλεία

Για την πραγματοποίηση της ανάλυσης χρησιμοποιήθηκε η μέθοδος CRAMM που δημιουργήθηκε από την Υπηρεσία ασφαλείας της Βρετανικής κυβέρνησης, καθώς και το βοηθητικό λογισμικό "The CRAMM Manager" της εταιρίας Insight Consulting, στην έκδοση 5.1. Η μέθοδος αυτή βασίζεται στην ποιοτική (qualitative) ανάλυση κινδύνων, όπου ο υπολογισμός της πιθανότητας να συμβεί μια απειλή και της αξίας των περιουσιακών στοιχείων βασίζεται σε προκαθορισμένες κλίμακες. Το πλεονέκτημα της μεθόδου αυτής είναι η ελαχιστοποίηση του χρόνου της ανάλυσης χωρίς να επιβαρύνεται ιδιαίτερα η ακρίβεια των αποτελεσμάτων.

3.1.5 Ευχαριστίες

Σε αυτό το σημείο και χρησιμοποιώντας πρώτο ενικό θα ήθελα να ευχαριστήσω όλους όσους συνεργάστηκα εντός της εταιρίας και με βοήθησαν να αποκομίσω τα κατάλληλα δεδομένα και να προχωρήσω στην παρακάτω μελέτη. Όλο αυτό έγινε σε συνεργασία με τον υπεύθυνο του τμήματος μηχανογράφησης τον κύριο Πατουσάκη Γεώργιο , τον οικονομικό διευθυντή Βάκχο Κώστα , τον υπεύθυνο λογιστηρίου Ζάφο Γεώργιο , την υπεύθυνο ανθρώπινου δυναμικού Κουλούρη Σοφία , τον προγραμματιστή του τμήματος μηχανογράφησης Παπανικόλα Παναγιώτη , τον υπεύθυνο του εμπορικού τμήματος Δηματά Γιάννη και την υπεύθυνο τιμολόγησης και αποθήκης Τσιτομάτη Ευαγγελία.

3.2.1 Επεξήγηση της μεθόδου CRAMM

Η μέθοδος CRAMM βασίζεται στην αναγνώριση και αξιολόγηση των περιουσιακών στοιχείων (assets) του οργανισμού, στην αναγνώριση και αξιολόγηση των απειλών που υπάρχουν προς αυτά, καθώς και την ευπάθεια τους προς τις συγκεκριμένες απειλές. Ο συνδυασμός αξίας – απειλών – ευπαθειών επιτρέπει τον υπολογισμό του βαθμού του κινδύνου (risk) που διατρέχει κάθε περιουσιακό στοιχείο προς κάθε συγκεκριμένη απειλή, με βάση μια κλίμακα κινδύνου. Με τον υπολογισμό αυτό φαίνεται ποιο στοιχείο/υπηρεσία κινδυνεύει και με ποιο τρόπο, ώστε να υιοθετούνται σωστοί και οικονομικοί (cost effective) τρόποι αντιμετώπισης. Επιπρόσθετα, η χρήση της κλίμακας του κινδύνου επιτρέπει τον προσδιορισμό προτεραιοτήτων στην υλοποίηση των αντιμέτρων.[2]

Η μέθοδος CRAMM αποτελείται από τα εξής στάδια:
- Αναγνώριση των περιουσιακών στοιχείων
- Δημιουργία ενός μοντέλου συσχέτισης μεταξύ τους
- Αξιολόγηση των περιουσιακών στοιχείων
- Αναγνώριση των απειλών προς τα περιουσιακά στοιχεία
- Αξιολόγηση της πιθανότητας να συμβεί μια απειλή καθώς και της ευπάθειας του κάθε περιουσιακού στοιχείου προς την απειλή αυτή
- Υπολογισμός του βαθμού κινδύνου
- Υπολογισμός των πιθανών αντίμετρων

Κάθε ένα από τα παραπάνω βήματα θα αναλυθεί παρακάτω σε συνδυασμό με τα αποτελέσματα που βρέθηκαν κατά την ανάλυση της εταιρίας X Medicals.

3.2.2 Περιουσιακά στοιχεία (assets)

Μεθοδολογία

Τα περιουσιακά στοιχεία που αναλύονται με την μέθοδο CRAMM μπορούν να χωριστούν σε πέντε κατηγορίες:

Δεδομένα (Data assets):
Στην κατηγορία αυτή ανήκουν κάθε είδους δεδομένα, από δεδομένα προσωπικού χαρακτήρα σε μια βάση δεδομένων μέχρι και οι καταχωρήσεις σε έναν DNS server.

Υπηρεσίες (End User Services):
Στην κατηγορία αυτή ανήκουν οι υπηρεσίες που επιτρέπουν στον τελικό χρήστη πρόσβαση στα δεδομένα. Για παράδειγμα η υπηρεσία πρόσβασης σε μια βάση δεδομένων που επιτρέπει στους χρήστες να προσπελάσουν τα δεδομένα που αυτή περιέχει.

Υλικά Στοιχεία:
Η κατηγορία αυτή περιλαμβάνει τα υλικά στοιχεία που αποτελούν το υπολογιστικό σύστημα, δηλαδή τους υπολογιστές, το δίκτυο, μέσα αποθήκευσης κτλ.

Τοποθεσίες:
Στην κατηγορία αυτή περιλαμβάνονται τα δωμάτια, κτίρια ή ακόμα και οικόπεδα τα οποία ανήκουν στον οργανισμό και περιέχουν μέρη των υπολογιστικών συστημάτων

Λογισμικό:
Η κατηγορία αυτή περιλαμβάνει το λογισμικό που χρησιμοποιείται από τους οργανισμούς. Η έννοια του λογισμικού είναι όταν το λογισμικό που χρησιμοποιείται είναι διαμορφωμένο με βάση της ανάγκες της κάθε εταιρίας και είναι υψίστης σημασίας η προστασία του κώδικα καθώς και τα παραγόμενα δεδομένα αυτού.

Τα περιουσιακά στοιχεία συσχετίζονται άμεσα μεταξύ τους.
Για παράδειγμα τα δεδομένα μιας βάσης δεδομένων συσχετίζονται με την υπηρεσία πρόσβασης της βάσης δεδομένων, με τον υπολογιστή που περιέχει την βάση δεδομένων , το λογισμικό καθώς και με το δωμάτιο που βρίσκεται αυτός ο υπολογιστής. Το μοντέλο αυτό μπορεί να επεκταθεί ακόμα περισσότερο και να περιλάβει το δίκτυο που χρησιμοποιείται για την μεταφορά των δεδομένων, τους προσωπικούς υπολογιστές των χρηστών που έχουν πρόσβαση στα δεδομένα καθώς και ότι άλλο θέλουμε να περιλάβουμε.

Η λογική της δημιουργίας του μοντέλου είναι ότι το κάθε στοιχείο μεταφέρει ή προσθέτει απειλές και ευπάθειες στο άλλο. Για παράδειγμα η εκδήλωση φωτιάς σε ένα δωμάτιο απειλεί τους υπολογιστές που περιέχονται σε αυτό, και επομένως και τις υπηρεσίες και δεδομένα που υπάρχουν στους υπολογιστές.

Τέλος, στην μέθοδο CRAMM τα περιουσιακά στοιχεία που αξιολογούνται είναι μόνο τα **δεδομένα** τα **υλικά στοιχεία** και το **λογισμικό** που χρησιμοποιείται σε κάθε περίπτωση. Θεωρείται ότι οι υπηρεσίες δεν έχουν αξία από μόνες τους, απλά περιέχουν την αξία των δεδομένων που προσφέρουν ή επεξεργάζονται.

Η αξιολόγηση των υλικών στοιχείων είναι απλή, καθώς υπολογίζεται η τρέχουσα οικονομική τους αξία με βάση κλίμακα που προκαθορίζεται από τη μέθοδο. Η αξιολόγηση των δεδομένων γίνεται με διαφορετικό τρόπο. Συγκεκριμένα, υπολογίζεται το αντίκτυπο που θα έχει στον οργανισμό η **μη διαθεσιμότητα, μη εξουσιοδοτημένη αποκάλυψη, μετατροπή** και **καταστροφή** των δεδομένων. Το αντίκτυπο που υπολογίζεται αντικατοπτρίζει πάντα την χειρότερη περίπτωση (worst case). Ο υπολογισμός του αντίκτυπου γίνεται με βάση κλίμακα από το 1 έως το 10 και με χρήση οδηγιών (guidelines) που περιέχει η μέθοδος. Οι οδηγίες αυτές περιέχουν κατάλογο με τους πιθανούς τύπους αντίκτυπων, ώστε να καλύπτονται όλες οι περιπτώσεις, καθώς δεν είναι πάντοτε δυνατός ο υπολογισμός του οικονομικού αντίκτυπου. Για παράδειγμα η απώλεια δεδομένων μπορεί να επιφέρει οικονομικό αντίκτυπο, νομικό αντίκτυπο, ηθικό αντίκτυπο (λόγω απώλειας προσωπικών δεδομένων), ακόμα και την απειλή ανθρώπινης ζωής σε ορισμένες περιπτώσεις. Στην αξιολόγηση του λογισμικού ακολουθείται και η προσέγγιση που έγινε με την αποτίμηση των υλικών στοιχείων αλλά και ο τρόπος που περιγράφτηκε για τα δεδομένα.

3.2.3 Αναγνώριση των περιουσιακών στοιχείων - X Medicals

Στην εταιρία X Medicals που γίνεται η πρακτική μελέτη και ύστερα από τη συνάντηση που έγινε με τον κύριο Χ υπεύθυνο του τμήματος μηχανογράφησης, τον κύριο Χ οικονομικό διευθυντή καταγράφθηκαν όλες οι κρίσιμες υπηρεσίες που έχουν άμεση συσχέτιση με την παραγωγική διαδικασία και τα πληροφοριακά συστήματα και το οποιαδήποτε πρόβλημα σε αυτές θα είχε επιπτώσεις στην σωστή λειτουργία του οργανισμού.

Με τη βοήθεια του υπεύθυνου του τμήματος μηχανογράφησης και ξεκινώντας, όπως αναφέρθηκε και παραπάνω, από τις υπηρεσίες, έγινε και ο καθορισμός των δεδομένων (Data), των φυσικών πόρων (Physical assets), των λογισμικών (Software assets) και των τοποθεσιών (Location).

Παρακάτω αναλύεται όλο το κύκλωμα της μελέτης αρχίζοντας από τις υπηρεσίες που περιλήφθηκαν στην διαδικασία της ανάλυσης κινδύνων

End of user Services

Authentication

Η υπηρεσία αυτή είναι καταλυτική για την εύρυθμη λειτουργία όλης της εταιρίας καθώς για οποιαδήποτε πρόσβαση στο πληροφοριακό σύστημα η οποιαδήποτε υπηρεσία που αναφέρεται παρακάτω ο κάθε χρήστης πρέπει να εισάγει το δικό του μοναδικό όνομα και κωδικό. Τα συστήματα που είναι διαθέσιμα στην X Medicals περιέχουν απόρρητα δεδομένα για την πρόσβαση των χρηστών στις υπηρεσίες που παρέχει (user account information).. Το ίδιο για την πρόσβαση εταιρία από το σπίτι του μέσω internet.

Back up

Η υπηρεσία αυτή προσκολλείται κυρίως στους servers της εταιρίας, στους οποίους έχει σχεδιαστεί να βρίσκονται όλα τα ευαίσθητα δεδομένα όπως βάσεις δεδομένων κοινόχρηστα αρχεία , ιατρικά δεδομένα , οικονομικής φύσεως στοιχεία, προσωπικά δεδομένα και πολλά άλλα. Η πολιτική της εταιρίας δεν επιτρέπει όλα αυτά τα απόρρητα και κρίσιμα δεδομένα να βρίσκονται σε συστήματα εκτός server. Επίσης αυτή η υπηρεσία αποτελείται από τρεις λειτουργίες. Η πρώτη είναι η γνωστή Tape Back up , όπου μέσα από την τεχνολογία των μαγνητικών ταινιών κρατιούνται όλα τα ζωτικά στοιχεία για τη λειτουργία του πληροφοριακού συστήματος αλλά και τα περισσότερο κρίσιμα δεδομένα(system state, db data, common files κτλ). Την ίδια δουλεία επίσης αλλά με ποιο λειτουργικό χρήσιμο και εύκολο τρόπο κάνει και η δεύτερη λειτουργία της Back up Υπηρεσίας ο Data Protection Manager (DPM). Ουσιαστικά κάνει την ίδια δουλειά με το Tape Back up , αλλά με μεγαλύτερη ευκολία. Βασισμένο στη νέα τεχνολογία η ανάκτηση χαμένων δεδομένων γίνεται πολύ πιο γρήγορα και ασφαλές από την πρώτη λειτουργία που αναφέραμε παραπάνω. Τέλος η Τρίτη λειτουργία είναι κυρίως για όλα τα κοινόχρηστα αρχεία αλλά και τα ευαίσθητα προσωπικά δεδομένα. Ονομάζεται Shadow copy και για όλα αυτά τα δεδομένα κρατάει καθημερινά κάποιες εκδώσεις ένας συγκεκριμένος server (File Server). Στην συγκεκριμένη περίπτωση το σύστημα κρατάει δύο εκδώσεις , μία 7 η ώρα το πρωί και μια στις 12 το μεσημέρι. Οποιαδήποτε αλλαγή γίνει στα αρχεία θα υπάρχει άμεσα μια δεύτερη έκδοση των αρχείων στην κατάσταση που ήταν τις συγκεκριμένες ώρες.

BS Strategy

Η υπηρεσία αυτή αναφέρεται στο εμπορική και οικονομική διεύθυνση της εταιρίας. Η συγκεκριμένη υπηρεσία αποτελείται από μια βάση δεδομένων και ένα λογισμικό το οποίο είναι ρυθμισμένο στις ανάγκες των διευθύνσεων. Πάνω σε αυτή την υπηρεσία γίνονται μελέτες και στατιστικές έρευνες πάνω στις πωλήσεις της εμπορικής διεύθυνσης, με σκοπό την δημιουργία στρατηγικών σχεδίων ανάπτυξης , μελέτη της αγοράς , και στοιχεία που απαρτίζουν τη γενικότερη εικόνα της εταιρίας πάνω σε αυτή.

DNS

Η διαθεσιμότητα της υπηρεσίας αυτής είναι απαραίτητη για την σωστή λειτουργία του δικτύου. Η μη διαθεσιμότητα της υπηρεσίας συνεπάγεται ουσιαστικά στην μη διαθεσιμότητα όλων των υπολογιστών , εξυπηρετητών , εκτυπωτών και άλλων στοιχείων του δικτύου μέσω της χρήσης διευθύνσεων dns.

EMAIL

Η υπηρεσία αυτή έχει δημιουργηθεί για την ευκολότερη επικοινωνία μεταξύ των εργαζομένων της εταιρίας αλλά και των πελατών που συνεργάζονται. Η υπηρεσία είναι διαθέσιμη μέσω ενός Exchange server που βρίσκεται εντός της εταιρίας και διαχειρίζεται από το τμήμα μηχανογράφησης.

ERP

Η υπηρεσία αυτή είναι η σημαντικότερη πάνω σε όλο το πληροφοριακό σύστημα της X Medicals. Είναι η σπονδυλική στήλη όλων των κύριων υπηρεσιών που παρέχει η εταιρία στους πελάτες αλλά και των υπηρεσιών που προσφέρει στους εργαζομένους ώστε να λειτουργούν πιο αποδοτικά. Πάνω σε αυτή δουλεύουν τα περισσότερα τμήματα της εταιρίας όπως το service , η αποθήκη , το τμήμα προσφορών , το τμήμα τιμολόγησης και το λογιστήριο. Επίσης είναι η πηγή δεδομένων για την BS Strategy υπηρεσία που αναφέρθηκε παραπάνω καθώς ότι δεδομένο επεξεργάζεται , προέρχεται από το ERP. Αποτελείτε και αυτή από μια ξεχωριστή βάση δεδομένων καθώς και με το λογισμικό της τα οποία βρίσκονται ξεχωριστά σε διαφορετικούς server.

Intranet

Το Intranet είναι μια υπηρεσία σε μορφή web η οποία δίνει τη δυνατότητα στους εργαζομένους να εργάζονται πάνω σε κοινά αρχεία , να ορίζονται ομάδες εργασίας με κοινά ημερολόγια , να έχουν την δυνατότητα για οποιαδήποτε αλλαγή συμβεί σε αρχεία που τους ενδιαφέρει να ενημερώνονται μέσω του mail. Ουσιαστικά είναι ένας δικτυακός τόπος αρχείων του οποίου ο χειρισμός γίνεται μέσα από μια ιστοσελίδα (admin / user) , υπάρχει ευκολία στην πρόσβαση , έλεγχος πρόσβασης για τον κάθε χρήστη, και για την κάθε ομάδα με άμεση ενημέρωση στα σημεία ενδιαφέροντος. Επίσης με την κατάλληλη πιστοποίηση και τα σωστά διαπιστευτήρια υπάρχει πρόσβαση και εκτός εταιρίας μέσω internet , ακόμα και από ένα κινητό τηλέφωνο προηγμένης τεχνολογίας.

Smart card

Η λειτουργία της υπηρεσίας αυτής είναι πολύ σημαντική καθώς επηρεάζει την πρόσβαση των εργαζομένων σε όλη την εταιρία και σχετίζεται άμεσα με την ασφάλεια του εξοπλισμού που περιέχεται (από κλοπή, καταστροφή κτλ). Κάθε χρήστης έχει μια Smart Card η οποία του δίνει πρόσβαση σε συγκεκριμένες φυσικές τοποθεσίες μέσα στην εταιρία , ανάλογος τον ρόλο του μέσα σε αυτή.

User File

Ο προσωπικός αποθηκευτικός χώρος των χρηστών, όπως και ο κοινόχρηστος χώρος που έχουν τα διάφορα τμήματα. Οι χώροι αυτοί βρίσκονται επίσης σε έναν κεντρικό server (File Server).

Τα συστήματα (υλικά στοιχεία) που υποστηρίζουν τις παραπάνω υπηρεσίες και περιλήφθηκαν στην ανάλυση παρουσιάζονται παρακάτω.

Physical Assets

Servers

APP_SRV Application Server : Είναι ο server στον οποίο βρίσκεται εγκατεστημένο το πρόγραμμα του ERP(Client - Server). Σε αυτόν γίνεται ο έλεγχος του licensing του προγράμματος για το ποιοί χρήστες μπορούν να το τρέξουν, πόσες άδειες και σε ποιες βάσεις έχει πρόσβαση ο κάθε ένας από αυτούς .

BACK_UP_DPM_SRV : Είναι ο Data Protector Manager server όπου διαχειρίζεται τα back up δεδομένα σε μία συστοιχία σκληρών δίσκων.

BACK_UP_TAPE_SRV : Είναι ο server που κρατάει τα back up δεδομένα στις λεγόμενες μαγνητικές ταινίες Tape.

DC_SRV (General Purpose Network Host) : Είναι ο Domain Controller του δικτύου και έχει βασική του ευθύνη την ομαλή λειτουργία όλου του δικτύου , το συγχρονισμό αυτού , την πολιτική του δικτύου μέσα από τους ρόλους που έχουν του ανατεθεί , την ασφάλεια για τις διαδικτυακές προσβάσεις των χρηστών (Log in , Checking permissions, κτλ) μέσα σε όλο το Domain. Υπάρχουν δύο servers που έχουν το ρόλο του domain controller , ένας βασικός και ένας additional σε περίπτωση που συμβεί κάτι στον πρώτο(Back up).

ERP_SRV (Database Server) : Είναι ο Database server οποίος έχει όλη τη βάση του ERP προγράμματος.

EXCH_SRV : Είναι ο server όπου αναλαμβάνει όλη τη διαδικασία του ηλεκτρονικού ταχυδρομείου της εταιρίας.

FILE_SRV File Server : Είναι ο server οπού βρίσκονται όλα τα αρχεία των χρηστών (προσωπικά αλλά και κοινόχρηστα δεδομένα) μέσα σε ένα storage, όπως επίσης και έχει έναν ρόλο της υπηρεσίας back up το shadow copy, που αναφέρθηκε παραπάνω.

SMART_CARD_SRV Database Server , Application Server : Είναι ο server ο οποίος έχει και την βάση δεδομένων αλλά και το λογισμικό που χρειάζεται για να λειτουργήσει ο έλεγχος και η ασφάλεια της εταιρίας σε θέματα φυσικών προσβάσεων.

WEB_SRV Intranet : Η κύρια λειτουργία αυτού του server είναι ακριβώς η διαχείριση εγγράφων (ηλεκτρονικών) με ενσωματωμένο versioning, full text search, metadata, permissions, ομαδοποιήσεις, tags και άλλα. Ουσιαστικά επιτρέπει την οργάνωση του εσωτερικού site της εταιρίας σε βιβλιοθήκες, subsites, security groups και άλλα.

Πριν συνεχιστεί η ανάλυση των physical assets του συστήματός είναι σημαντικό να σημειωθεί πως για την μελέτη θα γίνει έμφαση μόνο στα κύρια στοιχεία του συστήματος και όχι σε επιμέρους πχ απλά τερματικά, εκτυπωτές , καλώδια κτλ , διότι αυτά δεν θεωρήθηκαν άξια προς ανάλυση και από την ίδια την εταιρία αλλά και για τον σκοπό της μελέτης. Βέβαια επειδή είναι μέρος του συνολικού πληροφοριακού συστήματος απλοποιήθηκαν πριν εισαχθούν. Η απλοποίηση αυτή έγινε ως εξής. Επειδή σε κάθε τμήμα της εταιρίας όλοι έχουν την ίδια δουλειά και ασχολούνται με τα ίδια θέματα, αν κάποιο από αυτά αποτελούταν από τέσσερις θέσεις εργασίας με τέσσερις υπολογιστές και έναν εκτυπωτή στο σύστημα καταγραφόταν ως ένα workstation με ένα εκτυπωτή.

Παρακάτω παρουσιάζονται τα απλοποιημένα και ομαδοποιημένα workstations με βάση τη λειτουργικότητά τους

CRAMM - Physical Asset Workstation Review: X Medicals

	Workstation	Class	Number
Λογιστήριο	ACCOUNTING_DEP_WS	Workstation, Other Workstation	2
	Print Facilities	Printer	
Εμπορικό Τμήμα	COMMERCIAL_DEP_WS	Workstation, Other Workstation	3
	Workstation	Portable	
	Print Facilities	Printer	
Εξυπηρέτηση πελατών	CUST_SERV_WS	Workstation, Other Workstation	3
	Print Facilities	Printer	
	Peripheral Devices	Fax Machines	
Μηχανογράφηση	IT_WS	Workstation, Portable	2
	Workstation	Other Workstation	
	Print Facilities	Printer	
Διοίκηση	MANAGEMENT_WS	Workstation, Other Workstation	2
	Print Facilities	Printer	
	Workstation	Portable	
	Peripheral Devices	Fax Machines	
Υποδοχή	RECEPTION_WS	Print Facilities, Printer	2
	Workstation	Other Workstation	
Τεχνική Υποστήριξη	SERVICE_WS	Workstation, Portable	1
	Print Facilities	Printer	
	Workstation	Other Workstation	
Αποθήκη	WAREHOUSE_WS	Workstation, Personal Digital Assistant (PDA)	2
	Print Facilities	Printer	
	Workstation	Other Workstation	

Επιπλέον εκτός από τα workstations , υπάρχουν και μερικά physical assets τα οποία είναι ζωτικής σημασίας για το πληροφοριακό σύστημα της εταιρίας και παραθέτονται παρακάτω.

Physical Asset	Class		Number
ADSL_ROUTER	Network Distribution Component		
Storage Device	Magnetic Tape Device		1
IBM_STORAGE	Storage Device	Storage Device	1
SC_DEV_ACCOUNTING	Media	Electronic	1
SC_DEV_COMPUTER_ROOM	Media	Electronic	1
SC_DEV_ENTRANCE	Media	Electronic	1
SC_DEV_MANAGEMENT	Media	Electronic	1
SC_DEV_SERVICE	Media	Electronic	1
SC_DEV_WAREHOUSE	Media	Electronic	1
SWITCH	Network Distribution Component		3

Αφού έχει γίνει η αναγνώριση των υπηρεσιών και των φυσικών στοιχείων , στη συνέχεια γίνεται και η αναγνώριση των δεδομένων (Data) , του λογισμικού (Software) και των τοποθεσιών (Location)

DATA

Τα δεδομένα που παρουσιάζονται, αναφέρονται στις αντίστοιχες υπηρεσίες που αναφέρθηκαν Authentication Data, Back up Data, BS Data, DNS Data, EMAIL-pst Data (δεδομένα που βρίσκονται τοπικά σε κάθε υπολογιστή), EMAIL-box Data(δεδομένα που βρίσκονται στον Exchange server), ERP Data, Intranet DATA, Smart Card Data, User Files Data (ευαίσθητα προσωπικά δεδομένα), Common Files Data (κοινόχρηστα αρχεία) , Critical Data (ευαίσθητα οικονομικά δεδομένα)

Παρακάτω παρουσιάζεται ο πίνακας ομαδοποίησης των δεδομένων σε σχέση με τον τύπο τους.

DATA\TYPE	FINANCIAL	COMMERCIALLY SENSITIVE	SAFETY RELATED	PERSONAL
AUTHENTICATION			√	
BACK UP			√	
BS		√		
DNS			√	
e-MAIL pst				√
e-MAIL box		√		
ERP	√			
INTRANET		√		
SMART CARD			√	
User Files				√
Common Files		√		
Critical Files	√			

Software Assets

Το λογισμικό που θα πάρει μέρος στην ανάλυση αποτελείται από τα εξής :

BS strategy SW, ERP SW, SMART CARD SW

Location

Οι φυσικές τοποθεσίες που περιλαμβάνονται στην ανάλυση και αναφέρονται σε όλα τα παραπάνω είναι οι εξής :

X_Medicals , Athens, Accounting Department, Commercial Department

Computer Room, Customer Service, IT, Management, Reception

Service, Warehouse, Commercial Departmen

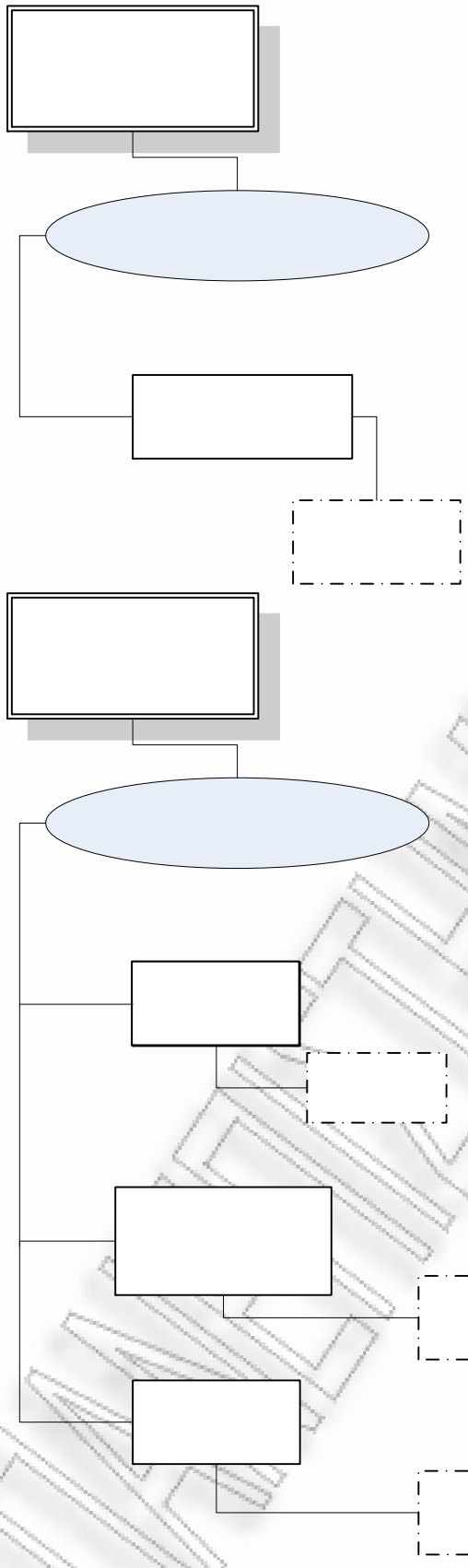
Στο Παράρτημα Α παρουσιάζεται αναλυτικά η αξιολόγηση και η ανάλυση του πληροφοριακού συστήματος της X Medicals μέσα από τις αναφορές της CRAMM.

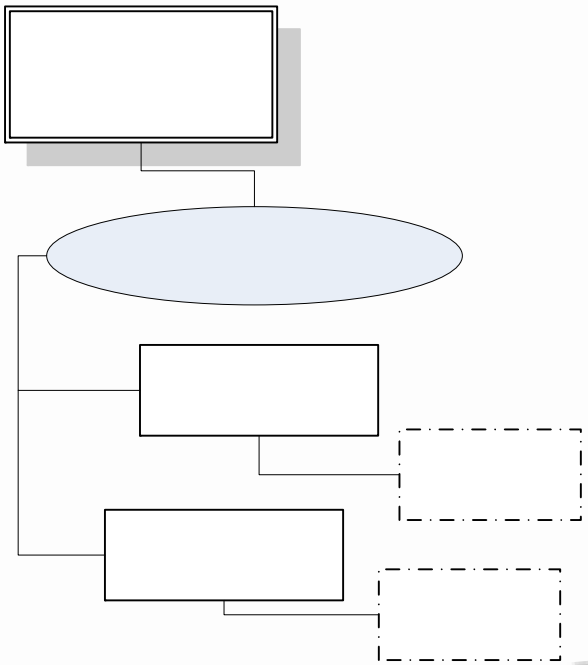
3.3 Μοντέλο Συσχέτισης

Αυτό το στάδιο είναι ένα πολύ σημαντικό σημείο για την εξέλιξη της μελέτης πάνω στα συστήματα της CRAMM αλλά και για μία συνοπτική και δομημένη απεικόνιση της όλης συλλογής των στοιχείων που έχει γίνει για την μελέτη του πληροφοριακού συστήματος.

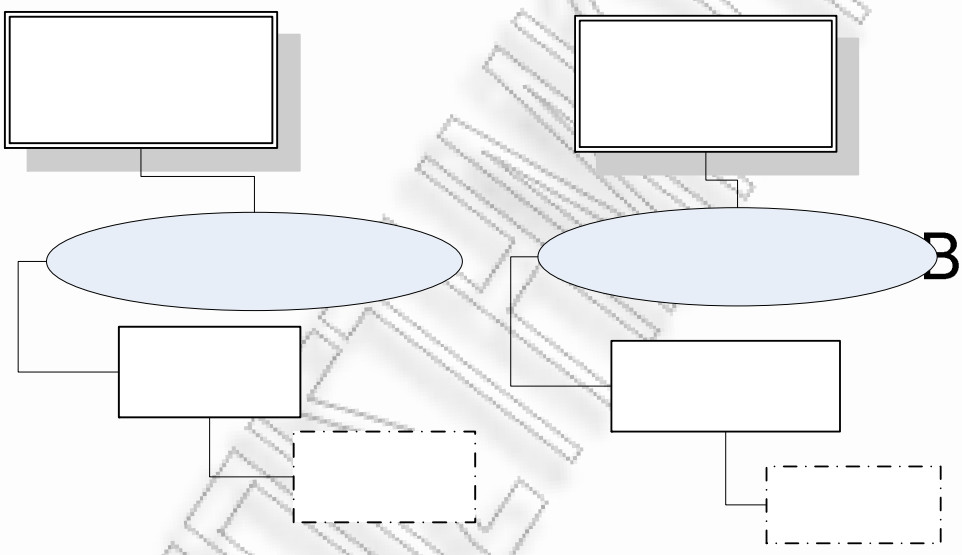
Η δημιουργία του μοντέλου γίνεται συσχετίζοντας τα δεδομένα-*Data* με τις υπηρεσίες τελικού χρήστη-*End of users Services* και με το υλικό που τις υποστηρίζει - *Physical assets* και αυτό με τη σειρά του με τις τοποθεσίες στις οποίες βρίσκεται-*Location*.

Το μοντέλο συσχέτισης για την ανάλυση της εταιρίας X Medicals φαίνεται παρακάτω.





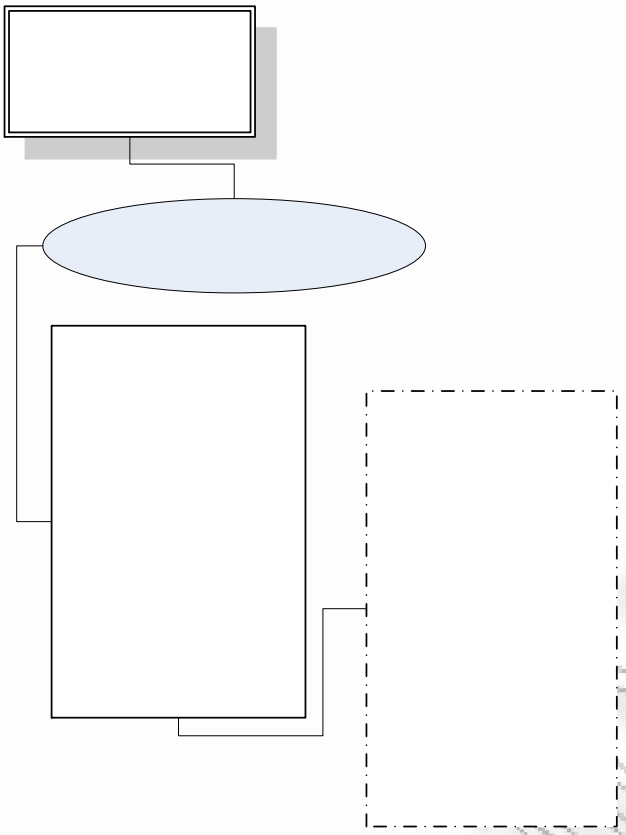
BS STRATEGY DATA



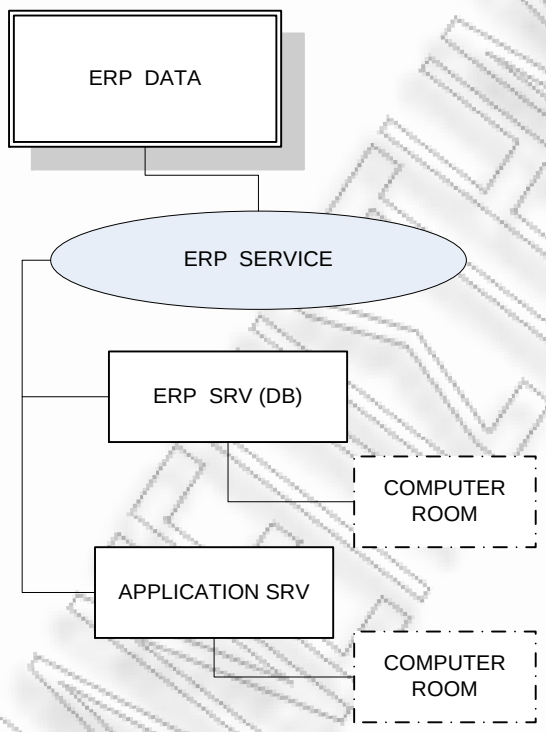
BS STRATEG

ERP SR

APPLICATION



EMAIL pst DATA



EMAIL SERV

ACCOUNTING_DEP_W

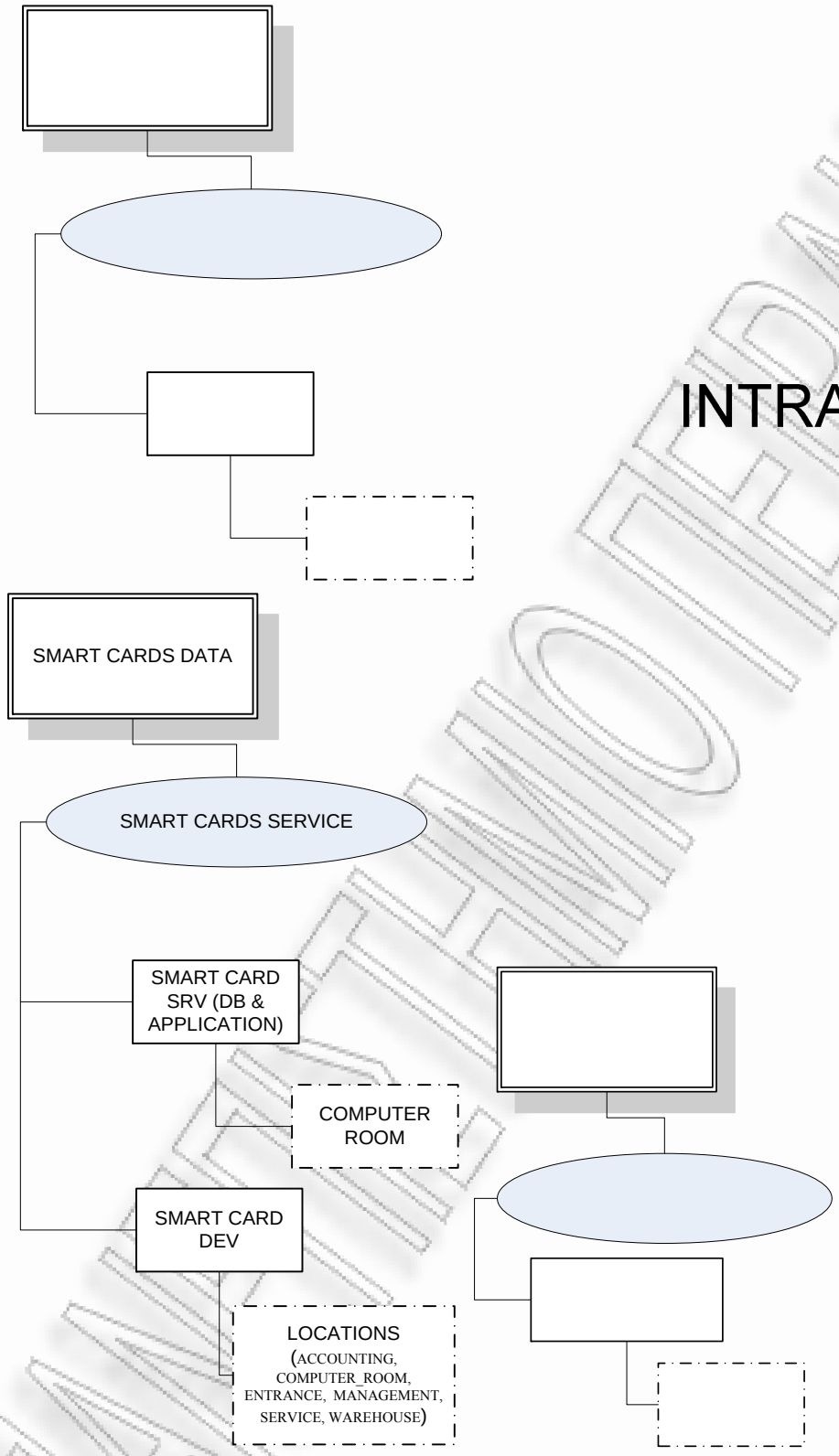
COMMERCIAL_DEP_W

CUST_SERV_WS,

IT_WS,

MANAGEMENT_WS

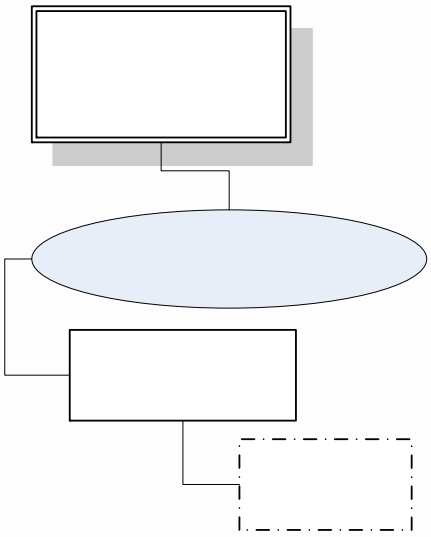
RECEPTION_WS,



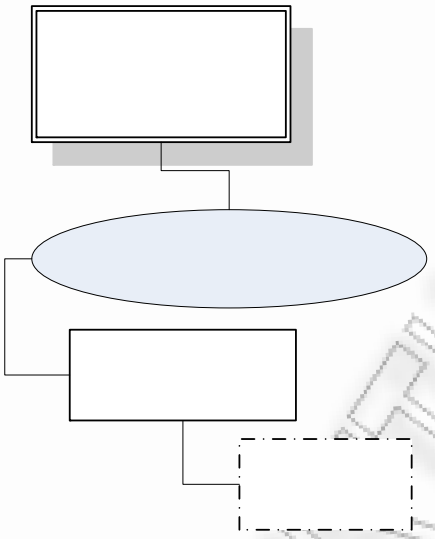
INTRANET DATA

INTRANET

WEB S



COMMON FILES DATA



USER FILES SERV

FILE SRV

Σημείωση

Η CRAMM θεωρεί τις υπηρεσίες ένα πολύ σημαντικό κομμάτι της μοντελοποίησης και δεν επιτρέπει την κατασκευή μοντέλων χωρίς υπηρεσίες. Σε περίπτωση που παραλειφθεί η δημιουργία του μοντέλου η ανάλυση προχωράει λαμβάνοντας υπόψη απομονωμένα τα αγαθά και τελικά το αποτέλεσμα θα είναι η πρόταση αποσπασματικών αντίμετρων. [2]

CC

3.4.1 Αξιολόγηση-Αποτίμηση περιουσιακών στοιχείων

Έχοντας δημιουργήσει το μοντέλο συσχέτισης το επόμενο βήμα είναι η αξιολόγηση των περιουσιακών στοιχείων της εταιρίας, η οποία γίνεται σε τέσσερα στάδια. Στα τρία πρώτα στάδια γίνεται η αποτίμηση των δεδομένων , των φυσικών αγαθών και των αγαθών λογισμικού. Τέλος στο τέταρτο στάδιο γίνεται ο υπολογισμός της έμμεσης αξίας των παραπάνω.

3.4.2 Αποτίμηση αγαθών δεδομένων

Σε αυτό το στάδιο, γίνεται η αποτίμηση των δεδομένων για κάθε επίπτωση με την κατάλληλη τιμή και βάση την μελέτη του πληροφοριακού συστήματος και του πίνακες επιπτώσεων της CRAMM. Στις περιπτώσεις όπου η απώλεια διαθεσιμότητας, ως επίπτωση, κρίνεται σημαντική για την μελέτη, η CRAMM συστήνει να ορίζονται τουλάχιστον τρεις τιμές, και ο ορισμός για τις υπόλοιπες περιπτώσεις γίνεται αυτόματα από το πρόγραμμα. Στη συγκεκριμένη μελέτη κάθε ομάδα δεδομένων έχει αντιμετωπιστεί κατά αυτό τον τρόπο , δηλαδή ξεκινώντας με βάση τη χειρότερη επίπτωση που μπορεί να έχει στην εταιρία ,και σύμφωνα πάντα με τις συνεντεύξεις που έδωσαν τα αρμόδια πρόσωπα αλλά και συμπερασματικά μελετώντας όλο το σύνολο των επιπτώσεων. Επίσης ορίστηκαν και τιμές στα ενδιάμεσα στάδια της κάθε περίπτωσης, ώστε να υπάρχει μια λογική συνέχεια μέχρι την τελική επίπτωση που επιλέχθηκε.

Ανάλυση Αποτίμησης

Η αξιολόγηση των δεδομένων καθώς και η αποτίμηση έγινε κυρίως σε συνεργασία με τον υπεύθυνο του τμήματος μηχανογράφησης τον κύριο Πατουσάκη Γεώργιο , την υπεύθυνο ανθρώπινου δυναμικού Κουλούρη Σοφία και τον προγραμματιστή του τμήματος μηχανογράφησης Παπανικόλα Παναγιώτη. Η επιλογή των συγκεκριμένων παραπάνω ατόμων έγινε πρώτιστα με την υπεύθυνο ανθρώπινου δυναμικού διότι γνωρίζει όλη την ροη και το βαθμό εργασίας για κάθε τμήμα της εταιρίας καθώς και την κρισιμότητα όλων αυτών. Επίσης σε συνάρτηση με τη βοήθεια τόσο του προγραμματιστή όσο και του υπεύθυνου μηχανογράφησης έγινε η συνοχή των δεδομένων και των μηχανογραφικών διαδικασιών πάνω στην ροή των εργασιών που αφορά την συγκεκριμένη ανάλυση,

Όπως αναφέρθηκε και παραπάνω η μελέτη για την αποτίμηση των δεδομένων έγινε σε συνάρτηση με τους πίνακες επιπτώσεων της CRAMM. Δηλαδή , με γνώμονα την κάθε πιθανή κατάσταση των δεδομένων έγινε η εκτίμηση της επίπτωσης και σε τι βαθμό η επιρροή της. Ξεκινώντας με την σειρά που τα παραθέτει το πρόγραμμα της CRAMM έγινε η εκτίμηση με βάση την Απώλεια διαθεσιμότητας Δεδομένων (>15 Λεπτών , > 1 Ώρας , >3 Ώρες ,…, 1 Εβδομάδας, κτλ) , την Μερική απώλεια και Ολική καταστροφή Δεδομένων , Αποκάλυψη των δεδομένων, Ύπαρξη λαθών στα δεδομένα , Σκόπιμη αλλοίωση των δεδομένων και ούτω κάθε εξής. Σε πολλές περιπτώσεις για κάθε κατάσταση υπήρχαν 2 ή και περισσότερες επιπτώσεις για την εταιρία, αλλά πάντα γινόταν η επιλογή αυτής με το μεγαλύτερο βαθμό επιρροής.

Για τη συνοπτική και ουσιώδες παρουσίαση όλων των αγαθών-δεδομένων χωρίστηκε όλη η μελέτη σε τρία στάδια. Το αρχικό στάδιο όπου εμφανίζονται οι πρώτες επιπτώσεις , στο μεσαίο στάδιο στο οποίο η κατάσταση έχει «επιδεινωθεί» με τις ίδιες επιπτώσεις σε μεγαλύτερο βαθμό ή και με διαφορετικές επιπτώσεις , και στο τελικό στάδιο όπου λήφθηκε υπόψη το ποια είναι η χειρότερη πιθανή επίπτωση και από ποια κατάσταση μπορεί να προέλθει. Επίσης είναι σημαντικό να σημειωθεί πως όλα τα δεδομένα έχουν την δική τους ιδιαίτερη κατάσταση για αυτό το λόγο μπορεί κάποιο να έχει μεγαλύτερη επίπτωση σε μια κατάσταση , όπου κάποια άλλα στην ίδια κατάσταση να έχουν πολύ μικρότερες επιπτώσεις.

3.4.3 Ομαδοποίηση της ανάλυσης με βάση τον τύπο των δεδομένων

Safety Related Data

Σε αυτή την ομάδα δεδομένων αντιστοιχούν τα Authentication , Dns , Back Up και Smart Card Data. Τα δύο πρώτα , όπως είναι κατανοητό, είναι απαραίτητα για την ομαλή λειτουργία και ασφάλεια όλου του δικτύου , κάνοντας βέβαια ξεχωριστή δουλεία το κάθε ένα , αλλά έχοντας σχεδόν τις ίδιες επιπτώσεις στην εταιρία σε ίδιες καταστάσεις. Τα Back Up δεδομένα ουσιαστικά χρησιμεύουν σε περιπτώσεις επαναφοράς δεδομένων ή κατάστασης συστημάτων των μηχανών, είτε για κάποια εξυπηρέτηση των χρηστών σε περιπτώσεις αλλοίωσης η διαγραφής δεδομένων , για κάποιες μετρήσεις που μπορεί να χρειαστούν, χωρίς να γίνει πάνω σε δεδομένα που χρησιμοποιούνται άμεσα και θα δημιουργήσουν ίσως δυσκολίες στην ροή των εργασιών. Τέλος τα δεδομένα smart card είναι δεδομένα που αφορούν τον έλεγχο πρόσβασης σε σημαντικές τοποθεσίες της εταιρίας και σε κυρίως οι επιπτώσεις είναι μετρήσιμες και ανάλογες σε βάθος χρόνου. Όσο δεν υπάρχει έλεγχος και περιορισμός σε βάθος χρόνου μπορεί οι επιπτώσεις να είναι από έλλειψη εμπιστοσύνης του προσωπικού μέχρι και οικονομικές απώλειες.

Financial Data

Σε αυτή την ομάδα δεδομένων αντιστοιχούν τα ERP και Critical Data , τα οποία λειτουργικά μέσα από τα μηχανογραφημένα συστήματα τις εταιρίας έχουν διαφορετική υπόσταση αλλά συμβαδίζουν ως σε ένα σημείο (τα δύο πρώτα στάδια) σε επιπτώσεις με σχεδόν ίδιες καταστάσεις. Τα ERP δεδομένα «ζουν» μέσα στο βασικό κορμό λειτουργιών του πληροφοριακού συστήματος, συνεπώς οποιαδήποτε επίπτωση και αν έχουν , κρίνεται επικίνδυνη για τη συνέπεια της σωστής λειτουργίας αυτού. Η παραμικρή μη διαθεσιμότητα δεδομένων αποφέρει δυσλειτουργία στην ροή των εργασιών. Η ροή συνήθως είναι κυκλική οπότε αν παρεμποδιστεί σε ένα σημείο είναι πολύ πιθανό να υπάρξει παρεμπόδιση των διαδικασιών στα επόμενα βήματα. Για παράδειγμα ένα πρόβλημα που μπορεί να εμφανιστεί σε διαδικασίες της αποθήκης αρχικά να επηρεάσει μόνο αυτό το τμήμα αλλά σταδιακό θα πάρει μέρος στα περισσότερα τμήματα της εταιρίας. Αυτό μεταφέρεται και εκτός εταιρία στη συνέχεια με τη μη εξυπηρέτηση του κοινού και με οικονομικές συνέπειες. Επίσης λόγω του ότι καταχωρούνται και όλα τα λογιστικά δεδομένα , μισθωτήρια και πολλά οικονομικά

στοιχεία ζωτικής σημασίας η επικινδυνότητα μπορεί να φτάσει και σε σημεία νομικών ζητημάτων.

Critical Data

Τα Critical Data είναι αρχεία τα οποία διαχειρίζονται μόνο τα στελέχη της διοίκησης και αποτελούνται κυρίως από οικονομικά στοιχεία , σχέδια δράσης , στρατηγικά πλάνα , αξιολογήσεις προσωπικού και ότι άλλο έχει σχέση με την εικόνα της εταιρίας και το περιβάλλον στον οποίο αναπτύσσεται . Είναι λοιπόν σημαντικά δεδομένα για την λειτουργία της διοίκησης και για αυτό το λόγω οι διάφορες επιπτώσεις έχουν ως αποτέλεσμα τη δυσλειτουργία της.

Commercially Sensitive Data

Σε αυτή την ομάδα δεδομένων αντιστοιχούν τα BS (Business Strategy) , e-mail box , Intranet και Common Files Data. Εκτός από τα BS data , τα υπόλοιπα παίρνουν μέρος ουσιαστικά για τον ίδιο σκοπό, με διαφορετική βέβαια υπόσταση.

Ξεκινώντας με τα δεδομένα που αφορούν την εφαρμογή Business Strategy και σημειώνοντας πως αυτά δεν επιδέχονται είτε αλλαγές είτε διαγραφές μέσα από το ίδιο το πρόγραμμα ,γίνεται αντιληπτό πως είναι θεωρητικά τα ποιο ασφαλή δεδομένα. Πηγή προέλευσης αυτών είναι τα ERP data που με τα κατάλληλα φίλτρα και με συγκεκριμένη επεξεργασία παρουσιάζονται στην εφαρμογή Business Strategy. Συνεπώς η αξιοπιστία των ERP data έχουν και την σημασία τους και για έναν ακόμη μηχανισμό λειτουργίας στην εταιρία. Αυτό το σημείο συνοχής των δύο διαφορετικών δεδομένων μπορεί να λειτουργήσει και ως παράγοντας ελέγχου για την αξιοπιστία του ERP από τη στιγμή που ένα λάθος στα δεδομένα γίνει αντιληπτό από τους χρήστες του Business Strategy. Επίσης είναι αξιοσημείωτο πως τα δεδομένα αυτά έρχονται από αντιγραφή του back up αρχείου της βάσης δεδομένων του ERP. Συνεπώς η μη διαθεσιμότητα των δεδομένων θα οφείλεται στην μη διαθεσιμότητα του back up της βάσης του ERP, δηλαδή άλλος ένας παράγοντας ελέγχου, αυτή τη φορά για τα back up data. Με βάση λοιπόν όλα τα παραπάνω οι πιθανές επιπτώσεις είτε λάθος δεδομένων είτε μη διαθεσιμότητας , είναι η επεξεργασία και οι μετρήσεις λάθος δεδομένων – αναφορών και η διακοπή των εργασιών του εμπορικού τμήματος και της διοίκησης στην εφαρμογή αντίστοιχα.

Τα υπόλοιπα Commercially Sensitive δεδομένα έχουν πιο απλή δομή και ουσιαστικά είναι τα αρχεία που διαμοιράζονται οι υπάλληλοι μεταξύ τους αλλά και με εκτός εταιρίας , εργασιακής φύσεως συνεργάτες. Τα e mail box data είναι ένα μέρος αυτών και κυρίως αυτών που βγαίνουν εκτός εταιρίας, όπως είναι κατανοητό. Αυτά βρίσκονται στον εξυπηρετητή που προσφέρει την υπηρεσία του email και βρίσκονται σε πρόγραμμα καθημερινού back up. Τα Intranet δεδομένα είναι αυτά που μοιράζονται διατμηματικά στην εταιρία και η πρόσβασή τους είναι εφικτή μέσω web τεχνολογίας. Κάθε αρχείο, ή λίστα αρχείων έχει την δική του παραμετροποιημένη ασφάλεια ώστε η πρόσβαση να ελέγχεται και να είναι η κατάλληλη για τους εξουσιοδοτημένους υπάλληλους. Η ασφάλειά τους καθορίζεται και δίνεται από το τμήμα μηχανογράφησης έπειτα από έγκριση της διοίκησης.

Τέλος τα Common Files δεδομένα είναι τα κοινόχρηστα αρχεία του κάθε τμήματος και πρόσβαση έχει μόνο αυτό. Τα Common Files και τα Intranet data επειδή χρησιμοποιούνται κατά τη διάρκεια της ημέρας συνέχεια παίρνουν μέρος σε δύο διαδικασίες back up. Η πρώτη είναι η προαναφερθείσα του καθημερινού back up και η δεύτερη η διαδικασία του shadow copy back up, η οποία γίνεται δύο φορές την ημέρα και κρατάει back up δύο εκδώσεις. Η μια είναι 8 η ώρα το πρωί και η άλλη δώδεκα το μεσημέρι. Αυτό γίνεται για την άμεση πρόσβαση των δεδομένων σε τυχών λάθη χρηστών. Συνεπώς οι επιπτώσεις αυτών των δεδομένων κυμαίνονται πάλι κυρίως σε διακοπή λειτουργιών σε περιπτώσεις μη διαθεσιμότητας.

Personal Data

Σε αυτή την ομάδα δεδομένων αντιστοιχούν τα e mail pst και τα user files,τα οποία όπως είναι κατανοητό αποτελούν τα προσωπικά αρχεία των υπαλλήλων και αρχεία που τους διευκολύνουν για το πέρας των εργασιακών καθηκόντων. Σε αυτό το σημείο πρέπει να αναφερθεί πως ως προσωπικά αρχεία θα έπρεπε να είναι τα αρχεία που δεν αφορούν εργασιακά καθήκοντα, το οποίο όμως είναι αδύνατο να ελεγχθεί απόλυτα παρά μόνο με την εργασιακή συνείδηση του κάθε υπαλλήλου. Αυτό οφείλεται στην συνεχόμενη και εντατική πίεση του χρόνου - φόρτου εργασίας αλλά και της αμεσότητας – ευκολίας που τα παρέχεται μέσα από τα προσωπικά αρχεία αλλά και από τη δομή του πληροφοριακού συστήματος. Τα email pst data είναι σε μορφή email και βρίσκονται αποθηκευμένα σε αρχεία pst διαχειριζόμενα μέσα από μια εφαρμογή γραφείου , η οποία δεν λήφθηκε υπόψη ως μέρος του εξεταζόμενου πληροφοριακού συστήματος. Τα user files είναι αρχεία διαφόρων τύπου υποστηριζόμενα πάλι από εφαρμογές γραφείου , τα οποία λαμβάνουν την ίδια αντιμετώπιση στη συγκεκριμένη μελέτη. Συνήθως αυτά τα δεδομένα έχουν την επικινδυνότητα της καταστροφής , της μη διαθεσιμότητας και της εξέθεσής τους εκτός εταιρίας, εξαιτίας λαθών του ιδίου του χρήστη από αμέλεια και από άγνοια λειτουργίας των συστημάτων που χρησιμοποιούν. Παρόλα αυτά οι επιπτώσεις σε αυτές τις περιπτώσεις δεν είναι καθόλου αμελητέες διότι εμφανίζουν εμπόδια στην εργασία , πολλές φορές δημιουργούν την αίσθηση της απογοήτευσης αλλά και τη δυνατότητα υποκλοπής αρχείων λόγω της μη ασφαλής θέσης τους.

Συνοψίζοντας λοιπόν όλη την παραπάνω ανάλυση για την αποτίμηση των δεδομένων παραθέτεται ο παρακάτω πίνακας , όπου μέσα από τα τρία στάδια που αναφέρθηκαν, φαίνονται τα πιθανά αποτελέσματα της επικινδυνότητας που εκτιμήθηκε.

DATA\ΕΠΙΠΤΩΣΗ	Αρχικό στάδιο	Μεσαίο στάδιο	Τελικό στάδιο
Safety Related Data			
AUTHENTICATION	Policy and Operation of Public Service	Disruption to activities / Financial Loss	Security & Intelligence
BACK UP	Management & Business Operations	Management & Business Operations	Management & Business Operations
DNS	Policy and Operation of Public Service	Disruption to activities / Financial Loss	Security & Intelligence
SMART CARD	Disruption to activities	Security & Intelligence	Financial Loss
Financial Data			
ERP	Disruption to activities	Policy and Operation of Public Service / Financial Loss	Law Enforcement
Critical Files	Disruption to activities	Disruption to activities	Management & Business Operations
Commercially Sensitive Data			
BS	Disruption to activities	Management & Business Operations	Commercial & Economic Interest
e-MAIL box	Disruption to activities	Disruption to activities / Loss of Goodwill	Policy and Operation of Public Service
INTRANET	Disruption to activities / Loss of Goodwill	Management & Business Operations	Commercial & Economic Interest
Common Files	Disruption to activities	Disruption to activities	Management & Business Operations
Personal Data			
e-MAIL pst	Disruption to activities	Disruption to activities / Loss of Goodwill	Commercial & Economic Interest
User Files	Disruption to activities	Disruption to activities / Loss of Goodwill	Commercial & Economic Interest

3.4.4 Αποτίμηση φυσικών αγαθών

Το στάδιο της αποτίμησης των υλικών – φυσικών αγαθών διαφέρει κατά πολύ από το στάδιο αποτίμησης δεδομένων. Δεν υπάρχουν πλέον κίνδυνοι και επιπτώσεις που θα καθορίσουν την αξία. Το μόνο που γίνεται σε αυτό το στάδιο είναι ο καθορισμός της αξίας του κάθε αγαθού- υλικού. Η αποτίμηση και αξιολόγηση των φυσικών αγαθών έγινε με την βοήθεια του υπεύθυνου τμήματος μηχανογράφησης Πατουσάκη Γεώργιο και με βάση την κλίμακα που περιλαμβάνεται στην CRAMM

Στη συνέχεια παραθέτεται ενδεικτικά ο πίνακας με την κλίμακα που χρησιμοποιεί η CRAMM

Βαθμός	Εύρος Τιμής €
1	1 έως 1.000
2	1.000 – 10.000
3	10.000 – 30.000
4	30.000 – 100.000
5	100.000 – 300.000

Κάνοντας λοιπόν την αξιολόγηση , παρατηρήθηκε πως τα περισσότερα υλικά αγαθά ανήκουν στη δεύτερη κλίμακα (1.000 έως 10.000 €) παρά μόνο οι συσκευές ελέγχου κάρτας smart cart devices όπου βρίσκονται στην πρώτη κλίμακα (1έως 1.000 €) και το workstation του εμπορικού τμήματος που βρίσκεται στην τρίτη κλίμακα (10.000 έως 30.000 €) και αυτό λόγω του ότι είναι το τμήμα με τους περισσότερους υπαλλήλους. Δεν παρουσιάζει δηλαδή κάποια ιδιαίτερα χαρακτηριστικά σε σχέση με τα άλλα workstation , απλά έχει αγαθά σε μεγαλύτερη ποσότητα.

<u>Σημείωση</u>

Η αξία των φυσικών αγαθών γίνεται με την αξία που αγοράστηκαν εφόσον είναι αρκετά πρόσφατα – καινούργια. Κανονικά η αξία που πρέπει να εισάγεται για όλα τα υλικά αγαθά να είναι η αξία αντικατάστασης των ήδη υπάρχων, και όχι να εισάγονται οι τιμές που αγοράστηκαν. *[2]*

Στον παρακάτω πίνακα φαίνεται πιο αναλυτικά τα φυσικά αγαθά που λαμβάνουν μέρος στο πληροφοριακό σύστημα της X Medicals με την ποσότητα , την αξία τους και τέλος το βαθμό που έχουν στην κλίμακα της CRAMM.

Physical Asset	Class	Quant.	Cost	Scale
Accounting Workstation	Workstation	2	3.600	2
ADSL Router	Modem	1	4.000	2
APP_SRV	Host-Application Server	1	5.000	2
Storage Device	Other Storage Device	1	3.200	2
Storage Device	Magnetic Tape Device	1	3.000	2
Commercial Dep. Workstation	Workstation	3	12.000	3
Customer Service Workstation	Workstation	3	1.800	2
DC_SRV	General Purpose Network Host	2	4.600	2
ERP_SRV	Host-Database Server	1	5.000	2
EXCH_SRV	Host-Other Host	1	5.800	2
FILE_SRV	Host-File Server	1	3.000	2
IBM_STORAGE	Storage Device	1	3.500	2
IT workstation	Workstation	2	3.000	2
Management Workstation	Workstation	2	2.800	2
Reception Workstation	Workstation	2	1.300	2
SC_DEV_(ACCOUNTING - COMPUTER_ROOM-ENTRANCE- MANAGEMENT- SERVICE- WAREHOUSE)	Other Electronic Media	1	400	1
Service Workstation	Workstation	1	1.000	1
Host	Application Server	1	2.500	2
SWITCH	Network Distribution Component-Switch	3	1.800	2
Warehouse Workstation	Workstation	2	4.000	2
WEB_SRV	Host-Other Host	1	2.000	2

3.4.5 Αποτίμηση αγαθών λογισμικού

Στο στάδιο αποτίμησης του λογισμικού ακολουθήθηκε η ίδια προσέγγιση με αυτή της αποτίμησης των δεδομένων, δηλαδή , η αξιολόγηση έγινε σε συνάρτηση με τους πίνακες επιπτώσεων της CRAMM. Για κάθε πιθανή κατάσταση της κάθε εφαρμογής έγινε η εκτίμηση της επίπτωσης και σε τι βαθμό η επιρροή της. Η αξιολόγηση αυτή έγινε κυρίως σε συνεργασία με τον υπεύθυνο του τμήματος μηχανογράφησης τον κύριο Πατουσάκη Γεώργιο.

Στην συγκεκριμένη μελέτη εξετάζονται τρεις εφαρμογές ,από τις οποίες οι δύο (ERP , Business Strategy) αποτελούν τον βασικό κορμό των λειτουργιών της X Medicals και η τρίτη (Smart Card) δρα ως έλεγχος ασφαλείας κρίσιμων φυσικών τοποθεσιών μέσα σε αυτή.

Ξεκινώντας με τη βασική εφαρμογή , που πάνω σε αυτή στηρίζεται το μεγαλύτερο κομμάτι της εταιρίας , το ERP , γίνεται κατανοητό πως η παραμικρή επίπτωση που μπορεί να εμφανιστεί μπορεί να έχει άμεσα και σε μεγάλο βαθμό επιρροή στην ροή των εργασιών. Όπως αναφέρθηκε και στην αποτίμηση των δεδομένων ERP , η ροή των εργασιών της εφαρμογής περιλαμβάνει τα περισσότερα τμήματα της εταιρίας. Συνεπώς η μη διαθεσιμότητα της εφαρμογής από λίγο χρονικά διάστημα (15 λεπτών) μέχρι και σε μεγάλο έχει ανάλογες επιπτώσεις στην διακοπή σημαντικών ενεργειών. Βέβαια πολλές από τις εργασίες αυτές μπορούν να γίνουν χειρόγραφα , χωρίς την ύπαρξη κάποιου πληροφοριακού συστήματος ή εφαρμογής , αλλά ο χρόνος υλοποίησης αυτών αυξάνεται κατά πολύ. Σε περιπτώσεις είτε μακροχρόνιας μη διαθεσιμότητας είτε μερικής και ολικής καταστροφής της εφαρμογής είναι πιθανό να υπάρξουν και νομικά ζητήματα , λόγω του ότι υπάρχουν δεδομένα λογιστικά και μισθοδοτικά , αλλά σύμφωνα με τη γνώμη του υπεύθυνου μηχανογράφησης είναι σχεδόν αδύνατο να συμβεί.

Η δεύτερη εφαρμογή το Business Strategy είναι ένα σημαντικό εργαλείο κυρίως για το τμήμα πωλήσεων και για τη διοίκηση. Είναι παραμετροποιημένο από εξωτερική εταιρία με βάση της ανάγκες της εταιρίας και αντλεί τα δεδομένα του μέσω ενός αρχείου back up της βάσης του ERP. Δεν είναι εφικτή η παραμετροποίηση του από τους χρήστες παρά μόνο από τους διαχειριστές (τμήμα μηχανογράφησης ή εξωτερική εταιρία) , όπως δεν είναι και εφικτή η τροποποίηση των δεδομένων που επεξεργάζεται. Η μη διαθεσιμότητα αυτής προκαλεί διακοπή εργασιών όπως έλεγχος πωλήσεων , στατιστικές μελέτες και οργάνωση στρατηγικών σχεδίων δράσης κυρίως για την ανάπτυξη της εταιρίας στο τμήμα πωλήσεων.

Η τρίτη εφαρμογή (Smart Card) δεν παίρνει μέρος όσο αναφορά τις λειτουργίες της εταιρία στο παραγωγικό κομμάτι, αλλά είναι σημαντική γιατί προσθέτει, στα ήδη υπάρχοντα, ένα επιπλέον μέτρο ασφαλείας στις περισσότερες τοποθεσίες της εταιρίας. Η μη διαθεσιμότητά της δεν εμποδίζει την συνέχεια της ροής των εργασιών , απλά προσθέτει μια αίσθηση ανασφάλειας των τμημάτων, στα οποία δεν πρέπει να υπάρχει γενική πρόσβαση , όπως αποθήκη, service , computer room , μηχανογράφηση , λογιστήριο και διοίκηση κυρίως τις ώρες εκτός εργασίας. Η αντικατάσταση της σε περιπτώσεις ολικής και μερικής καταστροφής δεν αποτελεί επιπλέων κίνδυνο και σύμφωνα με τον υπεύθυνο μηχανογράφησης είναι άμεσα εφικτή.

Παρακάτω παραθέτεται ο συνοπτικός πίνακας των εφαρμογών ανά επίπτωση χωρισμένος σε τρία στάδια , με την ίδια λογική που ακολουθήθηκε στον πίνακα αποτίμησης δεδομένων.

ΕΦΑΡΜΟΓΗ\ΕΠΙΠΤΩΣΗ	Αρχικό στάδιο	Μεσαίο στάδιο	Τελικό στάδιο
ERP	Disruption to activities	Disruption to activities / Financial Loss	Law Enforcement
BS Strategy	Disruption to activities	Disruption to activities / Management & Business Operations	Disruption to activities / Management & Business Operations
Smart Card	Security & Intelligence	Management & Business Operations	Security & Intelligence

3.4.6 Υπολογισμός έμμεσης αξίας

Στο τέταρτο και τελευταίο στάδιο γίνεται η διαδικασία υπολογισμού της έμμεσης αξίας. Η διαδικασία αυτή γίνεται αυτόματα από την CRAMM χωρίς να μπορεί να επέμβει σε αυτό το σημείο κάποιος ανθρώπινος παράγοντας. Ουσιαστικά κάνει μια εκτίμηση της αξίας των φυσικών αγαθών και των τοποθεσιών με βάση την αποτίμηση των δεδομένων και του λογισμικού. Δηλαδή, έχοντας στηριχθεί στο μοντέλο συσχέτισης, έχουν καθοριστεί όλοι οι σύνδεσμοι μεταξύ των στοιχείων που συσχετίζονται (τοποθεσία – φυσικό αγαθό – λογισμικό - δεδομένα) και πάνω σε αυτό γίνεται η εφαρμογή αντίμετρων πάνω στα φυσικά αγαθά και στις αντίστοιχες τοποθεσίες που βρίσκονται αυτά. Είναι μια λειτουργία προστασίας των δεδομένων και του λογισμικού καθώς τα φυσικά αγαθά είναι αυτά που επεξεργάζονται τα δεδομένα μέσα από τις εφαρμογές και φιλοξενούνται από τις συγκεκριμένες τοποθεσίες. Η γενικότερη φιλοσοφία που εφαρμόζει η CRAMM σε αυτό το σημείο είναι πως, όταν μια απώλεια συνεπάγει περισσότερες, τότε ο βαθμός της επίπτωσής της, θα προκύπτει από το μεγαλύτερο βαθμό αυτής, των συνεπαγόμενων

Υπολογίζοντας και την έμμεση αξία , ουσιαστικά κλείνει και το πρώτο μέρος της αξιολόγησης και αποτίμησης των αγαθών και ανοίγει το επόμενο μέρος, στο οποίο γίνεται εκτίμηση απειλών και αδυναμιών – ευπαθειών.

3.5.1 Εκτίμηση Απειλών και Ευπαθειών

Σε αυτό το στάδιο γίνεται η αναγνώριση των διαφόρων απειλών που πιθανόν να υπάρχουν προς κάθε περιουσιακό στοιχείο της X Medicals. Η CRAMM προσφέρει ένα μεγάλο εύρος απειλών, από τις οποίες γίνεται η επιλογή. Συγκεκριμένα , εξετάζοντας τα περιουσιακά στοιχεία κάθε ένα ξεχωριστά ,γίνεται και η αντιστοίχηση όλων των απειλών που ταιριάζουν και έχουν λογική συνοχή. Οι απειλές, όπως και τα περιουσιακά στοιχεία, χωρίζονται στις ανάλογες κατηγορίες , απειλές προς δεδομένα , φυσικά αγαθά, υπηρεσίες και τοποθεσίες. Βέβαια μπορεί να γίνει η κατηγοριοποίηση αυτών με βάση το περιεχόμενο τους, όπως Λογική διείσδυση (logical infiltration) - Επικοινωνιακή διείσδυση (communications infiltration) - Αποτυχία εξοπλισμού (failures of equipment) - Φυσικές Απειλές (physical threats) πχ. φωτιά, πλημύρα κτλ.

Μετά το πέρας της αντιστοίχησης των απειλών γίνεται η αξιολόγηση της πιθανότητας να συμβεί μια απειλή σε κάθε περιουσιακό στοιχείο, καθώς και η ευπάθεια του προς την απειλή αυτή. Η κάθε απειλή μπορεί να βαθμολογηθεί με τιμές very low , low , medium , high και very high , ενώ η ευπάθεια ενός περιουσιακού στοιχείου προς μια απειλή βαθμολογείται με τιμές low, medium και high.

Σαν μια πιο τυποποιημένη μορφή όλων των παραπάνω , είναι αντιληπτό πως το μέγεθος της πιθανότητας(ενδεχόμενο) είναι ανάλογο και με τη σημαντικότητα της απειλής σε συνάρτηση με το μέγεθος της ευπάθειας προς αυτή.

Πιθανότητα = *Απειλή x Ευπάθεια*

Η πιθανότητα αυτή , με τη σειρά της, καθορίζει ,αναλόγου μεγέθους , και την επικινδυνότητα που μπορεί να εκτεθεί το πληροφοριακό σύστημα , σε συνάρτηση πάντα με την επίπτωση.

Επικινδυνότητα = *Πιθανότητα x Επίπτωση*

Στη συνέχεια, για την ολοκλήρωση της αξιολόγησης , γίνεται ομαδοποίηση των αγαθών , ανάλυση και συσχέτιση των απειλών και τέλος εκτίμηση επιπέδων απειλών και ευπαθειών για να είναι έτοιμη η CRAMM στο τέλος αυτών και μέσα από συγκεκριμένες διαδικασίες να κάνει τον υπολογισμό της επικινδυνότητας.

3.5.2 Ομαδοποίηση

Η ομαδοποίηση των αγαθών του πληροφοριακού συστήματος, χρειάζεται για να γίνει καλύτερα ο συσχετισμός αυτών με τις απειλές που διαθέτει η CRAMM. Η ομαδοποίηση δεν είναι κατά ανάγκη υποχρεωτική. Μπορεί να μην γίνεται ομαδοποίηση μεταξύ κάποιων , να μην ωφελεί σε κάποια μεμονωμένα αγαθά ή μπορεί να χρειαστεί κάποια από αυτά να μετρηθούν μόνα τους. Επίσης ο συσχετισμός που γίνεται με τις απειλές εξαρτάται πάλι στον αναλυτή της κάθε μελέτης, δηλαδή μπορεί να υπάρχουν κάποιες απειλές στις οποίες να μην χρειαστεί να γίνει συσχετισμός λόγω του ότι δεν ενδιαφέρει την μελέτη , όπως και επίσης να μην μπορεί να γίνει κάποιος συσχετισμός εκ φύσεως, π.χ. απειλές φυσικών καταστροφών σε δεδομένα. Στην συγκεκριμένη μελέτη η ομαδοποίηση των αγαθών έγινε κυρίως σε φυσικά αγαθά και λιγότερο σε δεδομένα , εφαρμογές και υπηρεσίες, διότι η πληθώρα των φυσικών αγαθών που μελετήθηκε ήταν πολύ μεγαλύτερη από τα υπόλοιπα και προσέφερε αυτή τη δυνατότητα.

Η ομαδοποίηση των φυσικών αγαθών έγινε στις μονάδες ελέγχου των Smart Card για όλες τις τοποθεσίες που βρίσκονταν, στα workstations όλων των τμημάτων , στο hardware του networking εξοπλισμού (modem – router , switches) και σε ένα μεγάλο κομμάτι εξυπηρετητών “Blade Center” το οποίο περιλαμβάνει του εξής : ERP_srv , EXCH_srv , FILE_srv, WEB_srv και IBM storage. Όλα αυτά λειτουργούν ως virtual machines σε ένα μεγάλο server με κοινό storage.

Η ομαδοποίηση των δεδομένων περιορίστηκε στα DNS και Authentication data και χαρακτηρίστηκε ως Domain_operation data και στα Common Files , Intranet data ως TEAM data files.

Ομαδοποίηση των εφαρμογών και των υπηρεσιών δεν έγινε καθώς δεν θεωρήθηκε αναγκαία για το συσχετισμό των απειλών που θα παρουσιαστούν παρακάτω.

3.5.3 Συσχέτιση

Το κομμάτι της συσχέτισης των απειλών με τα αγαθά ή τις ομάδες αγαθών που δημιουργήθηκαν, η CRAMM δίνει την δυνατότητα να γίνει με δύο τρόπους. Ο πρώτος γίνεται με το συσχετισμό μια απειλής σε ένα ή περισσότερα αγαθά (ή ομάδες) και ο δεύτερος με το συσχετισμό ενός αγαθού (ή ομάδας) σε μια ή περισσότερες απειλές. Στην συγκεκριμένη μελέτη κρίθηκε πιο βολικός ο πρώτος , δηλαδή σε κάθε απειλή που διαθέτει η CRAMM να συσχετίζεται και το αντίστοιχο αγαθό.

Απειλή **Masquerading of User Identity by Insiders**

Η απειλή της μεταμφίεσης της ταυτότητας χρήστη από υπαλλήλους της εταιρίας επηρεάζει αρκετά από τα αγαθά του πληροφοριακού συστήματος. Πρώτα από όλα την υπηρεσία πιστοποίησης των χρηστών σε κάθε ενέργεια και σε κάθε τομέα δικαιοδοσίας που έχει ο χρήστης. Π.χ. στην περίπτωση που ένας χρήστης εκτός του τμήματος λογιστηρίου γνωρίζει τον κωδικό κάποιου που ανήκει στο τμήμα , τότε μπορεί να εκμεταλλευτεί ότι προσβάσεις και ενέργειες μπορεί να έχει με βάση αυτόν τον κωδικό. Με βάση αυτό έχει την δυνατότητα να αποκτήσει πρόσβαση σε αρχεία του ιδίου χρήστη , σε κοινόχρηστα αρχεία του τμήματος (Intranet και Team data Files) που ανήκει , να τα υποκλέψει , να τα τροποποιήσει , να τα διαγράψει και πολλά άλλα , χωρίς όμως να αφήνει ίχνη προσωπικά, παρά μόνο την κλεμμένη ταυτότητα που έχει χρησιμοποιήσει.

Επίσης μπορεί να αποκτήσει πρόσβαση και στον τοπικό υπολογιστή του "Θύματος" υποκλέβοντας προσωπικά αρχεία , και e mail. Υποκλέβοντας και χρησιμοποιώντας τους κωδικούς ERP μπορεί να αποκτήσει πρόσβαση και στα δεδομένα , έχοντας τη δυνατότητα αλλά και τη γνώση, να τα τροποποιήσει. Αποτέλεσμα αυτού είναι η τροποποίηση των δεδομένων του Business Strategy.

Άλλο ένα σημαντικό γεγονός που είναι πιθανό , είναι η χρησιμοποίηση της Smart Card. Έχοντας στα χέρια του κάποιος μια κάρτα άλλου χρήστη , αυτομάτως αποκτάει πρόσβαση και στα σημεία πρόσβασης που έχει η κάρτα με αποτέλεσμα όσες περισσότερες προσβάσεις έχει η κάρτα , τόσες και επιλογές ο μεταμφιεσμένος χρήστης.

Παρακάτω παραθέτεται ένας συνοπτικός πίνακας με τα επηρεαζόμενα αγαθά της συγκεκριμένης απειλής.

Masquerading of User Identity by Insiders
!AUTHENTICATION
!BS_DATA
!EMAIL-box_DATA
!EMAIL-pst_DATA
!ERP_DATA
!INTRANET
!INTRANET_DATA
!SMART_CARD
!USER_DATA
!USER_FILE
TEAM_DATA_FILES

Απειλή **Masquerading of User Identity by Contracted Service Providers**

Μια παρεμφερή απειλή με την προηγούμενη είναι αυτή της μεταμφίεσης της ταυτότητας από εξωτερικούς συνεργάτες. Στη συγκεκριμένη εταιρία , οι λόγοι που χρησιμοποιούν τις υπηρεσίες εξωτερικών εταιριών ή προσώπων είναι περιορισμένοι και σε λεπτά ζητήματα , με αποτέλεσμα να μην υπάρχει σε μεγάλο εύρος η πιθανότητα διείσδυσης καθώς παρακολουθούνται αυστηρά. Στα συστήματα λοιπόν που εμφανίζονται τέτοιες περιπτώσεις είναι τα email και κυρίως όταν υπάρχει κάποιο ιδιαίτερο τεχνικό πρόβλημα που δεν μπορεί να αντιμετωπιστεί από το τμήμα της μηχανογράφησης, στο ERP , που λόγω του ότι ο προγραμματιστής της εταιρίας είτε δεν έχει τις γνώσεις είτε τα εργαλεία για να ρυθμίσει κάποιο ζήτημα και δημιουργείται η ανάγκη του εξωτερικού συνεργάτη. Και επειδή οι περισσότερες ενέργειες των εξωτερικών συνεργατών απαιτούν και ορισμένες προσβάσεις σε τοπικούς υπολογιστές , είτε για ενημερώσεις είτε για παραμετροποίηση , υπάρχει και κίνδυνος να έρθουν σε επαφή με αρχεία χρηστών.

Παρακάτω παραθέτεται ο πίνακας με τα επηρεαζόμενα αγαθά της απειλής.

Masquerading of User Identity by Contracted Service Providers
!EMAIL
!ERP
!USER_FILE

Απειλή **Masquerading of User Identity by Outsiders**

Σε αυτή την απειλή το μόνο αγαθό που θεωρήθηκε ότι έχει άμεση συσχέτιση είναι η υπηρεσία της πιστοποίησης της κάρτας Smart Card. Υποκλέπτοντας μια κάρτα μπορεί κάποιος εκτός της εταιρίας να έχει φυσική πρόσβαση στην εταιρία. Μάλιστα σε ώρες εκτός λειτουργίας της εταιρίας μόνο συγκεκριμένες κάρτες έχουν την πρόσβαση για την είσοδο. Ακόμα σε περίπτωση κλοπής η απώλειας της κάρτας επιβάλλεται η άμεση ενημέρωση στην υπεύθυνο του ανθρώπινου δυναμικού και αύτη με τη σειρά της ενημερώνει το τμήμα μηχανογράφησης για να θέσει την συγκεκριμένη κάρτα ως ανενεργή , και να δημιουργηθεί μια νέα. Για τις ώρες εντός της λειτουργίας της εταιρίας υποχρεούται κάθε άτομο εκτός αυτής να συνοδεύεται.

Απειλή **Unauthorized Use of an Application**

Σε αυτή την απειλή "μη πιστοποιημένη χρήση εφαρμογής" η συσχέτιση γίνεται στις εφαρμογές Business Strategy και ERP . Στο Business Strategy ειδικότερα, εκτός ότι δεν είναι εφικτή η παραμετροποίηση των δεδομένων που επεξεργάζεται αλλά και η ίδια η εφαρμογή , υπάρχουν συγκεκριμένα προφίλ χρηστών με κωδικούς. Έτσι αν οποιοσδήποτε μη εξουσιοδοτημένος χρήστης προσπαθήσει να λειτουργήσει την εφαρμογή θα πρέπει να γνωρίζει κάποιο κωδικό από τα συγκεκριμένα προφίλ. Προσπερνώντας όλα αυτά τα εμπόδια , στο μόνο που μπορεί να ωφεληθεί είναι η συλλογή πληροφοριών με βάση της αναφορές που βγαίνουν μέσα από το πρόγραμμα.

Βέβαια αυτές οι πληροφορίες είναι οικονομικά στοιχεία των πωλήσεων που έχουν γίνει, και είναι αρκετά σημαντικές για τις ανταγωνιστικές εταιρίες του χώρου. Στην περίπτωση της εφαρμογής ERP , η μη εξουσιοδοτημένη πρόσβαση γίνεται άμεσα αντιληπτή από το τμήμα μηχανογράφησης , καθώς υπάρχει άμεση ενημέρωση από την ίδια την εφαρμογή και με συγκεκριμένες λεπτομέρειες. Επίσης όπως και στο Business Strategy που αναφέρθηκε παραπάνω , υπάρχουν συγκεκριμένα προφίλ για την πρόσβαση συγκεκριμένων βάσεων δεδομένων. Έχοντας παρακάμψει όλα τα παραπάνω ο χρήστης μπορεί να τροποποιήσει τα δεδομένα αλλά και την εφαρμογή χωρίς κανένα περιορισμό , το οποίο μπορεί να επιφέρει στην εταιρία αρκετές δυσάρεστες συνέπειες, νομικού περιεχομένου , διακοπή κρίσιμων λειτουργιών και πολλά άλλα.

Threat: Unauthorised Use of an Application
!BS_STRATEGY
!ERP

Απειλή **Introduction of Damaging or Disruptive Software**

Ο φόβος του κακόβουλου λογισμικού που μπορεί να εισβάλει σε κάποιο πληροφοριακό σύστημα με οποιονδήποτε τρόπο , ποτέ δεν ξεπεράστηκε τελείως. Ο λόγος , πως τα αντϊικά λογισμικά εξελίσσονται συνέχεια και πάντα προς το καλύτερο , επειδή συνεχώς εξελίσσονται και τα κακόβουλα λογισμικά. Σε αυτή την απειλή λοιπόν είναι πιθανό να κολλήσουν όλα τα μηχανήματα που είναι ενεργά πάνω στο δίκτυο της εταιρίας και περισσότερο αυτά στα οποία δουλεύουν οι χρήστες. Στα συστήματα της X Medicals υπάρχουν αντϊικά , ρυθμισμένα για καθημερινή ενημέρωση , καθημερινό και live έλεγχο. Βέβαια αυτό δεν σημαίνει πως είναι και ασφαλές.

Παρακάτω είναι ο πίνακας με τα φυσικά αγαθά που είναι πιθανό να επηρεαστούν.

Threat: Introduction of Damaging or Disruptive Software
!!Workstation
!BACK_UP_DPM_SRV
!BACK_UP_TAPE_SRV
!SMART_CARD_SRV
Blade_Center
Networking_HW

Απειλή **Misuse of System Resources**

Η κακή χρήση των πόρων των πληροφοριακών συστημάτων είτε από τη πλευρά των χρηστών είτε από την πλευρά της μηχανογράφησης έχει αποτελέσματα στα οποία σπάνια κανείς δίνει την απαραίτητη σημασία. Το παρακάτω παράδειγμα θα βοηθήσει στην κατανόηση των αποτελεσμάτων αυτών.

Έστω ότι ο υπάλληλος της εταιρίας έχει μία αμοιβή των χιλίων ευρώ το μήνα , που συνεπάγεται σε σαράντα ευρώ τη μέρα και πέντε ευρώ την ώρα. Εάν την μέρα συνολικά χάνει μιας ώρας δουλειάς λόγω της κακής χρήσης των πόρων του συστήματος τότε ετησίως υπάρχει απώλεια των 1.300 ευρώ, σύμφωνα με τον παρακάτω πίνακα. Σε μία εταιρία όπως η X Medicals που απασχολεί περίπου στους εκατό υπαλλήλους, το χρόνο θα έχει απώλεια 130.000 ευρώ.

Hourly Employee Cost	Daily Misuse (Hours)	Daily Loss Per Employee	Weekly Loss Per Employee	Annual Loss Per Employee
5 €	1	1x5=5€	5x5=25€	52x25=1.300€

Με βάση τα παραπάνω, γίνεται κατανοητό πως το αποτέλεσμα μιας ώρας χαμένης από κάθε υπάλληλο δεν είναι καθόλου αμελητέα. Για αυτό το λόγω και πρέπει να υπάρχει σωστή προσοχή στην χρήση των πόρων των πληροφοριακών συστημάτων.

Στην συγκεκριμένη μελέτη της εταιρίας X Medicals θα εξεταστούν μόνο τα φυσικά αγαθά που παίρνουν μέρος στο μεγαλύτερο κομμάτι της ροής των ενεργειών της εταιρίας, όπως είναι τα workstations , ο Blade Center και τα δικτυακά μηχανήματα (router & switches) .

Threat: Misuse of System Resources
!!Workstation
Blade_Center
Networking_HW

Απειλή **Communications Infiltration**

Η απειλή της διείσδυση επικοινωνιών σκοπεύει κυρίως στην υποκλοπή δεδομένων και έπειτα σε πιθανές αλλοιώσεις και καταστροφές αυτών. Συνεπώς είθισται να εμφανίζεται στις καίριες υπηρεσίες που παρέχει το πληροφοριακό σύστημα. Στην περίπτωση της X Medicals επιλέχθηκαν και οι κυριότερες υπηρεσίες όπως φαίνεται και στον παρακάτω πίνακα.

Threat: Communications Infiltration
!AUTHENTICATION
!BS_STRATEGY
!DNS
!EMAIL
!ERP
!INTRANET

Απειλή **Communications Failure**

Όπως και στην παραπάνω απειλή , η διακοπή των επικοινωνιών επηρεάζει άμεσα όλες της διαδικτυακές υπηρεσίες της εταιρίας και η διακοπή έστω και μίας μπορεί να αποφέρει διακοπή λειτουργιών πολλών τμημάτων μέσα σε αυτή. Ένας εύκολος στόχος για την επίτευξη αυτού είναι και τα δικτυακά (Networking) μηχανήματα που λειτουργούν ως φυσικός σύνδεσμός όλων των υπηρεσιών.

Threat: Communications Failure
!AUTHENTICATION
!BACK_UP
!BS_STRATEGY
!DNS
!EMAIL
!ERP
!INTRANET
!SMART_CARD
!USER_FILE
Networking_HW

Απειλή **Embedding of Malicious Code**

Η ενσωμάτωση κακόβουλου κώδικα συνήθως γίνεται από δεδομένα εκτός εταιρίας και πιθανός φορέας να είναι τα e mail , Internet – Intranet και στη συνέχεια οποιαδήποτε άλλα αρχεία που είτε είναι κοινόχρηστα είτε μπορούν εύκολα να μεταβιβαστούν εντός της εταιρίας.

Threat: Embedding of Malicious Code
!EMAIL
!INTRANET

Απειλή **Accidental Misrouting**

Η λανθασμένη δρομολόγηση δεδομένων συνήθως γίνεται από σφάλμα του χρήστη, λόγω της ανεπαρκής και κακής ίσως εκπαίδευσης των χρηστών. Τα ευαίσθητα δεδομένα θα πρέπει πάντα να είναι προστατευμένα και σε πολλές περιπτώσεις και κρυπτογραφημένα, και δεν θα πρέπει να υπάρχει έλλειψη της απόδειξης από την παραλαβή ενός μηνύματος. Συνήθως παρατηρούνται στα e mails αλλά και στο Intranet τέτοιου είδους λάθη.

Threat: Accidental Misrouting
!EMAIL
!INTRANET

Απειλή **Technical Failure of Host**

Η απειλή αυτή, όπως είναι κατανοητό προσπίπτει σε όλους του εξυπηρετητές του πληροφοριακού συστήματος της X Medicals. Σημαντική απειλή ειδικά όταν ένα σύστημα όπως ο Blade Center , που παρέχει το σύνολο των υπηρεσιών της εταιρίας.

Threat: Technical Failure of Host
!BACK_UP_DPM_SRV
!BACK_UP_TAPE_SRV
!SMART_CARD_SRV
Blade_Center

Απειλή **Technical Failure of Storage Facility**

Η μη λειτουργία ή η δυσλειτουργία του storage ενός συστήματος είναι ανάλογη και με τη χρήση που γίνεται στο συγκεκριμένο μέσο. Στην συγκεκριμένη περίπτωση λόγω του ότι πάνω στο IBM storage στηρίζονται όλες οι λειτουργίες του Blade Center καθιστά άκρως επικίνδυνο για την εταιρία η μη διαθεσιμότητά του αλλά και η δυσλειτουργία του.

Threat: Technical Failure of Storage Facility
Blade_Center

Απειλή **Technical Failure of Print Facility**

Η απώλεια των εκτυπωτικών εγκαταστάσεων είναι ένα σύνηθες φαινόμενο καθώς υπάρχει μια γενικότερη αμέλεια για της συντήρησής τους. Είναι μια σημαντική απειλή όσο αναφορά έγγραφες λειτουργίες, που δυστυχώς είναι αναπόσπαστο κομμάτι των περισσότερων τμημάτων.

Threat: Technical Failure of Print Facility
!!Workstation

Απειλή **Technical Failure of Network Distribution Component**

Όπως αναφέρθηκε και προηγουμένως , τα μέρη που αποτελούν το δικτυακό σύνδεσμο των υπηρεσιών ενός πληροφοριακού συστήματος , είναι άκρως σημαντικά. Οποιαδήποτε δυσλειτουργία τους ή μη διαθεσιμότητά τους είναι ύψιστης σημασίας για την ομαλή λειτουργία της εταιρίας.

Threat: Technical Failure of Network Distribution Component
Networking_HW

Απειλή **Technical Failure of Network Gateway**

Λόγω του ότι στην σημερινή εποχή η επικοινωνία , ενδοτμηματική ή εξωτερική, παίζει το σημαντικότερο ρόλο για την ολοκλήρωση των λειτουργιών στο ελάχιστο δυνατό του χρόνου, θα πρέπει να είναι λειτουργική και σταθερή. Το κυριότερο μέσω της επικοινωνίας με το εξωτερικό περιβάλλον της X Medicals είναι η email υπηρεσία , που απαιτεί την ύπαρξη του Internet.

Threat: Technical Failure of Network Gateway
!ADSL_ROUTER

Απειλή **Power Failure**

Η απειλή τις απώλειας ρεύματος σε κάθε πληροφοριακό σύστημα, πρέπει να αξιολογείται σωστά, ώστε να υπάρχει πάντα ένας τρόπος για την αποφυγή του κινδύνου αυτού. Η απειλή αυτή επαφίεται σε όλα τα φυσικά αγαθά που λειτουργούν με ρεύμα, και έχουν είτε άμεση είτε έμμεση σχέση με την λειτουργία των συστημάτων.

Threat: Power Failure
!!Workstation
!ACCOUNTING_DEP_WS
!BACK_UP_DPM_SRV
!BACK_UP_TAPE_SRV
!SMART_CARD_SRV
Blade_Center
Networking_HW

Απειλή **Air Conditioning Failure**

Οι προδιαγραφές λειτουργίας όλων των συστημάτων και ακόμη περισσότερο των μεγάλων και πολυσύνθετων πληροφοριακών συστημάτων απαιτούν την κατάλληλη προσοχή. Έτσι και οι θερμοκρασίες στις οποίες δουλεύουν τα συγκεκριμένα συστήματα δεν πρέπει να απέχουν από τις προδιαγραφές του κατασκευαστή. Για αυτό το λόγο πρέπει πάντα να δίνεται σημασία στην θερμοκρασία που βρίσκονται τα κεντρικά ηλεκτρονικά συστήματα και να παρατηρείται συστηματικά. Στην συγκεκριμένη μελέτη όλα τα κεντρικά συστήματα βρίσκονται σε μια τοποθεσία της εταιρίας "Computer Room" και η ύπαρξη κλιματιστικών καθίσταται απαραίτητη.

Threat: Air Conditioning Failure
Blade_Center
Networking_HW

Απειλή **System and Network Software Failure**

Όπως είναι κατανοητό η συγκεκριμένη απειλή μη διαθεσιμότητας δικτυακών συστημάτων είναι απόλυτα σημαντική και άξια προς μελέτη. Σε αυτή την απώλεια πάλι επαφίενται τα φυσικά αγαθά και αυτά που κυρίως έχει δικτυακή δραστηριότητα. Τα αποτελέσματα γίνονται αντιληπτά άμεσα , από την δυσλειτουργία μιας κάρτας ενός workstation μέχρι και το παραμικρό πρόβλημα σε θέματα routing και network load balancing.

Threat: System and Network Software Failure
!!Workstation
!BACK_UP_DPM_SRV
!BACK_UP_TAPE_SRV
!SMART_CARD_SRV
Blade_Center
Networking_HW

Απειλή **Application Software Failure**

Η μη διαθεσιμότητα μιας εφαρμογής σε μια εταιρία όπου ο κάθε της πόρος είναι σημαντικός αποτελεί δυσκινησία για την λειτουργία της. Έτσι αναλόγως και την κρισιμότητα της εφαρμογής υπάρχει και η ανάλογη δυσλειτουργικότητα στην εταιρία. Η μη διαθεσιμότητα του Business Strategy λοιπόν μπορεί να μην είναι τόσο σημαντική όσο του ERP αλλά δημιουργεί πολλά προβλήματα που σε βάθος χρόνου μπορούν να αποβούν άκρως επικίνδυνα. Το ίδιο ισχύει για την εφαρμογή της Smart Card , πόσο μάλλον και για το ERP που είναι ο βασικός κορμός των περισσότερων λειτουργιών της εταιρίας.

Threat: Application Software Failure
!BS_STRATEGY_SW
!ERP_SW
!SMART_CARD_SW

Απειλή **Hardware & Software Maintenance Error**

Η συντήρηση τόσο του λογισμικού όσο και των φυσικών αγαθών στο πληροφοριακό σύστημα είναι άκρως απαραίτητη. Για αυτό το λόγο λοιπόν θα πρέπει να γίνεται σε όλα τα συστήματα και με ιδιαίτερη προσοχή. Θα πρέπει να υπάρχει ο σωστός σχεδιασμός τους και σε ώρες που δεν θα υπάρχει παρεμπόδιση του έργου των υπαλλήλων.

Threat: Hardware Maintenance Error
!BACK_UP_DPM_SRV
!BACK_UP_TAPE_SRV
!IBM_STORAGE
Blade_Center

Threat: Software Maintenance Error
!BS_STRATEGY
!ERP
!SMART_CARD
Threat: User Error
!EMAIL-box_DATA
!EMAIL-pst_DATA
!ERP_DATA
TEAM_DATA_FILES
Threat: Fire
Blade_Center
Networking_HW

Απειλή **Theft by Insiders**

Η συγκεκριμένη απειλή κυρίως συναντάται σε φυσικά αγαθά αλλά και δεδομένα. Τα φυσικά αγαθά που κυρίως είναι εύκολα για κλοπή είναι αυτά που βρίσκονται στον χώρο του κάθε υπαλλήλου. Μπορεί να είναι ασήμαντα αλλά και αρκετά σημαντικά με έμμεσο ή άμεσο τρόπο. Η κλοπή ενός PDA έχει άμεσο κόστος στη εταιρία αλλά η κλοπή μιας κάρτας Smart Card δεν έχει, που βεβαίως αποτελεί έμμεσο κίνδυνο σε περιπτώσεις λάθους χειρισμού. Επίσης δεδομένα όπως τα κοινόχρηστα αρχεία μπορούν να αποφέρουν σημαντικές πληροφορίες για ανταγωνιστικές εταιρίες του χώρου , προκαλώντας οικονομικές απώλειες για την εταιρία.

Threat: Theft by Insiders
!!Media
!!Workstation
TEAM_DATA_FILES

Απειλή **Theft by Outsiders**

Η απειλή της κλοπής από εξωγενής παράγοντες είναι σημαντική αλλά δύσκολα εφικτή καθώς στη συγκεκριμένη εταιρία υπάρχει αυστηρός έλεγχος και παρακολούθηση των προσώπων που εισέρχονται σε αυτή ενώ δεν ανήκουν. Η πρόσβασή τους σε καίρια σημεία που μπορεί να αποφέρουν άσχημες καταστάσεις, κάνοντας υποκλοπή , γίνεται πάντα με συνοδεία καθώς απαιτείτε η κατοχή της κατάλληλης Smart Card.

Threat: Theft by Outsiders
!Commercial_Department
!Customer_Service
!Reception
!Warehouse

Απειλή **Willful Damage by Insiders & Outsiders**

Η απειλή της καταστροφής των αγαθών της εταιρίας από τους υπαλλήλους της είναι άμεση συνυφασμένη με την ηθική κατάσταση των υπαλλήλων της. Λόγω του ότι τα περισσότερα φυσικά αγαθά που μπορούν να καταστραφούν από αυτούς δεν έχουν μεγάλη οικονομική βαρύτητα για την εταιρία , δεν έχει δοθεί μεγάλης σημασίας πέραν των Smart Card. Αυτά που είναι άξια προσοχής , είναι τα δεδομένα που παρέχονται στους χρήστες. Η απειλή της καταστροφής των αγαθών της εταιρίας από πρόσωπα εκτός της εταιρίας είναι εφικτή σε σημεία που είναι πιθανόν να έχουν εύκολη πρόσβαση.

Threat: Willful Damage by Insiders
!!Media
!EMAIL-box_DATA
!EMAIL-pst_DATA
!ERP_DATA
TEAM_DATA_FILES

Threat: Willful Damage by Outsiders
!Commercial_Department
!Customer_Service
!Reception
!Warehouse

3.5.4 Αξιολόγηση

Η CRAMM διαθέτει δύο μεθόδους με τις οποίες μπορεί να γίνει η παραπάνω αξιολόγηση. Την ***ταχεία αξιολόγηση*** (rapid risk assessment) και την μέθοδο των ***ερωτηματολόγιων***. Κάθε μια από αυτές μπορεί να χρησιμοποιηθεί ή ακόμα και συνδυασμός των δύο.

Στην μέθοδο των ερωτηματολόγιων, η CRAMM παράγει ένα πλήθος ερωτημάτων για κάθε ζεύγος απειλής – περιουσιακού στοιχείου. Οι ερωτήσεις αυτές είναι τύπου πολλαπλών επιλογών, όπου η κάθε απάντηση βαθμολογείται με ορισμένο αριθμό πόντων. Με την απάντηση όλων των ερωτήσεων το πρόγραμμα προσθέτει τους βαθμούς που συλλέχτηκαν και υπολογίζει την απειλή και την ευπάθεια με μια από τις παραπάνω κλίμακες (low, high κτλ). Για να λειτουργήσει σωστά η μέθοδος, τα ερωτηματολόγια πρέπει να απαντηθούν από άτομα που γνωρίζουν πολύ καλά το περιουσιακό στοιχείο που αναλύεται, και πάντα με την βοήθεια ενός αναλυτή κινδύνων.

Η μέθοδος της ταχείας αξιολόγησης είναι πιο απλή και προφανώς πιο γρήγορη. Στην μέθοδο αυτή επιχειρείται να βρεθεί άμεσα ο βαθμός της απειλής ή της ευπάθειας με βάση οδηγίες (guidelines) που παρέχονται από την μέθοδο. Συγκεκριμένα, η απειλή βαθμολογείται για το πόσο συχνά μπορεί να επιφέρει μη διαθεσιμότητα, κλοπή, καταστροφή και μεταβολή των δεδομένων. Η ευπάθεια βαθμολογείται για την πιθανότητα να επέλθει η χειρότερη περίπτωση όταν πραγματοποιηθεί μια απειλή (*να σημειωθεί ότι η χειρότερη περίπτωση είχε υπολογιστεί κατά την αξιολόγηση των περιουσιακών στοιχείων*). Η μέθοδος αυτή απαιτεί, περισσότερο από την προηγούμενη, έμπειρα άτομα που γνωρίζουν πολύ καλά τα προβλήματα που υπάρχουν και μπορούν να κάνουν άμεσους υπολογισμούς των κινδύνων.

Για την αξιολόγηση εφαρμόστηκε η μέθοδος των ερωτηματολόγιων. Η όλη διαδικασία ολοκληρώθηκε με τη συνεργασία του υπεύθυνου του τμήματος μηχανογράφησης κύριο Πατουσάκη. Η εισαγωγή των δεδομένων αξιολόγησης στο πρόγραμμα έγινε επιτυχώς και παράχθηκαν τα αποτελέσματα που δίνονται στις επόμενες σελίδες. Για κάθε απειλή φαίνεται ο βαθμός της απειλής και της ευπάθειας του κάθε συστήματος προς αυτήν. Για καλύτερη κατανόηση δίνεται παρακάτω μια ενδεικτική «αποκωδικοποίηση» της κλίμακας της απειλής.

Η κλίμακα της απειλής αποκωδικοποιείται περίπου ως εξής:

very low - δεν αναμένεται να συμβεί συχνότερα από μια φορά κάθε 10 χρόνια
low - αναμένεται να συμβεί περίπου κάθε 3 χρόνια
medium - αναμένεται να συμβεί περίπου κάθε χρόνο
high - αναμένεται να συμβεί περίπου κάθε 4 μήνες
very high - αναμένεται να συμβεί περίπου κάθε μήνα

Ο βαθμός της ευπάθειας είναι ενδεικτικός για το πόσο εύκολα μπορεί να συμβεί μεγάλη ζημιά σε περίπτωση που συμβεί κάποιο επεισόδιο. Συγκεκριμένα, γνωστοποιεί πόσο πιθανό είναι να συμβεί η χειρότερη περίπτωση. Στους παρακάτω πίνακες παρουσιάζεται συνοπτικά ο βαθμός ευπάθειας και απειλής.

Masquerading of User Identity by Insiders	*Ευπάθεια*	*Απειλή*
!INTRANET	*Medium*	*Low*
!SMART_CARD	*Very Low*	*Low*
!AUTHENTICATION	*Low*	*Low*
!USER_FILE	*High*	*High*
!ERP_DATA	*Medium*	*Low*
!USER_DATA	*Very High*	*High*
!EMAIL-pst_DATA	*Medium*	*High*
!INTRANET_DATA	*Medium*	*High*
!BS_DATA	*Medium*	*Medium*
!EMAIL-box_DATA	*Very Low*	*Medium*
TEAM_DATA_FILES	*High*	*High*
Masquerading of User Identity by Contracted Service Providers		
!EMAIL	*Very Low*	*Medium*
!ERP	*Low*	*High*
!USER_FILE	*Very Low*	*High*
Communications Infiltration		
!EMAIL	*Low*	*Medium*
!INTRANET	*Very Low*	*Medium*
!ERP	*Medium*	*Medium*
!BS_STRATEGY	*Medium*	*Medium*
!DNS	*Very Low*	*Low*
!AUTHENTICATION	*Very Low*	*Low*

Masquerading of User Identity by Outsiders	*Ευπάθεια*	*Απειλή*
!SMART_CARD	*Medium*	*Medium*
Unauthorised Use of an Application		
!ERP	*Medium*	*High*
!BS_STRATEGY	*Low*	*Medium*
Introduction of Damaging or Disruptive Software		
!SMART_CARD_SRV	*Very Low*	*Low*
!!Workstation	*Medium*	*High*
!BACK_UP_TAPE_SRV	*Very Low*	*Low*
!BACK_UP_DPM_SRV	*Very Low*	*Low*
Networking_HW	*Very Low*	*High*
Blade_Center	*Very Low*	*High*
Misuse of System Resources		
!!Workstation	*Medium*	*High*
Networking_HW	*Medium*	*High*
Blade_Center	*Medium*	*Medium*
Embedding of Malicious Code		
!EMAIL	*High*	*Medium*
!INTRANET	*Low*	*Low*
Accidental Mis-routing		
!EMAIL	*Very Low*	*Low*
!INTRANET	*Very Low*	*Low*

Hardware Maintenance Error	*Ευπάθεια*	*Απειλή*
!BACK_UP_TAPE_SRV	*Low*	*High*
!BACK_UP_DPM_SRV	*Low*	*High*
!IBM_STORAGE	*Low*	*High*
Blade_Center	*Very Low*	*Medium*
Software Maintenance Error		
!ERP	*Low*	*High*
!BS_STRATEGY	*Low*	*Medium*
!SMART_CARD	*Very Low*	*Medium*

Theft by Insiders	*Ευπάθεια*	*Απειλή*
!!Workstation	*Medium*	*Medium*
!!Media	*Medium*	*Medium*
TEAM_DATA_FILES	*High*	*Low*
Theft by Outsiders		
!Warehouse	*Very Low*	*High*
!Reception	*Very Low*	*High*
!Customer_Service	*Very Low*	*High*
!Commercial_Department	*Low*	*Medium*

Communications Failure	*Ευπάθεια*	*Απειλή*
!EMAIL	*Very Low*	*High*
!INTRANET	*Low*	*High*
!ERP	*Low*	*High*
!BS_STRATEGY	*Very Low*	*High*
!SMART_CARD	*Very Low*	*High*
!BACK_UP	*High*	*High*
!DNS	*Very Low*	*High*
!AUTHENTICATION	*Very Low*	*High*
!USER_FILE	*Very Low*	*High*
Networking_HW	*Very Low*	*High*
Technical Failure of Print Facility		
!!Workstation	*Medium*	*Low*
Technical Failure of Network Distribution Component		
Networking_HW	*Low*	*Medium*
Application Software Failure		
!ERP_SW	*Very High*	*High*
!BS_STRATEGY_SW	*Very High*	*Low*
!SMART_CARD_SW	*Very Low*	*Medium*

Technical Failure of Host	*Ευπάθεια*	*Απειλή*
!SMART_CARD_SRV	*Low*	*Low*
!BACK_UP_TAPE_SRV	*Medium*	*Low*
!BACK_UP_DPM_SRV	*Low*	*Low*
Blade_Center	*Medium*	*Medium*
Technical Failure of Storage Facility		
Blade_Center	*Medium*	*Medium*
Technical Failure of Network Gateway		
!ADSL_ROUTER	*Low*	*Medium*
Power Failure		
!SMART_CARD_SRV	*High*	*Medium*
!!Workstation	*High*	*Medium*
!BACK_UP_TAPE_SRV	*High*	*Medium*
!BACK_UP_DPM_SRV	*High*	*Medium*
!ACCOUNTING_DEP_WS	*High*	*Medium*
Networking_HW	*High*	*Medium*
Blade_Center	*High*	*Medium*
Air Conditioning Failure		
Networking_HW	*Very Low*	*Medium*
Blade_Center	*Very Low*	*Medium*

Fire		
Networking_HW	*Low*	*High*
Blade_Center	*Very Low*	*High*
User Error		
!ERP_DATA	*Medium*	*Low*
!EMAIL-pst_DATA	*Very High*	*High*
!EMAIL-box_DATA	*Medium*	*Medium*
TEAM_DATA_FILES	*Medium*	*Medium*

System and Network Software Failure		
!SMART_CARD_SRV	*Very Low*	*Medium*
!!Workstation	*Very Low*	*Low*
!BACK_UP_TAPE_SRV	*Medium*	*High*
!BACK_UP_DPM_SRV	*Low*	*High*
Networking_HW	*Low*	*Medium*
Blade_Center	*Low*	*Medium*

Wilful Damage by Insiders		
!!Media	*Very Low*	*Low*
!ERP_DATA	*Very Low*	*Medium*
!EMAIL-pst_DATA	*Low*	*Low*
!EMAIL-box_DATA	*Low*	*Low*
TEAM_DATA_FILES	*Low*	*Low*

Wilful Damage by Outsiders		
!Warehouse	*Very Low*	*High*
!Reception	*Very Low*	*High*
!Customer_Service	*Very Low*	*High*
!Commercial_Department	*Very Low*	*High*

4 Υπολογισμός του κινδύνου

4.1 Μεθοδολογία

Ο υπολογισμός του βαθμού του κινδύνου με την μέθοδο CRAMM γίνεται με την χρήση ενός πίνακα «κινδύνου» ο οποίος παρέχεται. Η λογική πίσω από τον υπολογισμό είναι ο συνδυασμός των τιμών της αξίας, απειλής και ευπάθειας ώστε να παραχθεί ένα νούμερο που να είναι ενδεικτικό του «κόστους» που έχει στον οργανισμό η κάθε απειλή. Η κλίμακα του κίνδυνου στο CRAMM κυμαίνεται από το 1 (πολύ μικρός κίνδυνος) έως το 7 (πολύ μεγάλος κίνδυνος). Ο βαθμός αντικατοπτρίζει και το επίπεδο των απαιτήσεων ασφαλείας καθώς μεγάλος κίνδυνος υποδεικνύει υψηλές απαιτήσεις ασφαλείας.

Παρακάτω φαίνεται ο πίνακας «κινδύνου» βάση του οποίου γίνονται οι υπολογισμοί:

Threat	Very Low	Very Low	Very Low	Low	Low	Low	Medium	Medium	Medium	High	High	High	Very High	Very High	Very High
Vuln. Asset Value	LOW	MEDIUM	HIGH	LOW	MEDIUM	HIGH	LOW	MEDIUM	HIGH	LOW	MEDIUM	HIGH	LOW	MEDIUM	HIGH
1	1	1	1	1	1	1	1	1	2	1	2	2	2	2	3
2	1	1	2	1	2	2	2	2	3	2	3	3	3	3	4
3	1	2	2	2	2	3	2	3	3	3	3	4	3	4	4
4	2	2	3	2	3	3	3	3	4	3	4	4	4	4	5
5	2	3	3	3	3	4	3	4	4	4	4	5	4	5	5
6	3	3	4	3	4	4	4	4	5	4	5	5	5	5	6
7	3	4	4	4	4	5	4	5	5	5	5	6	5	6	6
8	4	4	5	4	5	5	5	5	6	5	6	6	6	6	7
9	4	5	5	5	5	6	5	6	6	6	6	7	7	7	7
10	5	5	6	5	6	6	6	6	6	6	7	7	7	7	7

4.2 Υπολογισμός του κινδύνου στην X Medicals

Το πρόγραμμα CRAMM υπολογίζει αυτόματα τον βαθμό του κινδύνου όταν ολοκληρωθούν τα προηγούμενα στάδια αξιολόγησης των περιουσιακών στοιχείων, απειλών και ευπαθειών. Τα περιληπτικά αποτελέσματα από την ανάλυση στην X Medicals φαίνονται στις παρακάτω σελίδες.

	Ευπάθεια	Απειλή	Κίνδυνος
Masquerading of User Identity by Insiders			
!INTRANET	*Medium*	*Low*	6
!SMART_CARD	*Very Low*	*Low*	2
!AUTHENTICATION	*Low*	*Low*	5
!USER_FILE	*High*	*High*	7
!ERP_DATA	*Medium*	*Low*	5
!USER_DATA	*Very High*	*High*	7
!EMAIL-pst_DATA	*Medium*	*High*	4
!INTRANET_DATA	*Medium*	*High*	6
!BS_DATA	*Medium*	*Medium*	6
!EMAIL-box_DATA	*Very Low*	*Medium*	5
TEAM_DATA_FILES	*High*	*High*	7
Masquerading of User Identity by Contracted Service Providers			
!EMAIL	*Very Low*	*Medium*	5
!ERP	*Low*	*High*	5
!USER_FILE	*Very Low*	*High*	5
Masquerading of User Identity by Outsiders			
!SMART_CARD	*Medium*	*Medium*	4
Unauthorized Use of an Application			
!ERP	*Medium*	*High*	6
!BS_STRATEGY	*Low*	*Medium*	5
Introduction of Damaging or Disruptive Software			
!SMART_CARD_SRV	*Very Low*	*Low*	2
!!Workstation	*Medium*	*High*	6
!BACK_UP_TAPE_SRV	*Very Low*	*Low*	1
!BACK_UP_DPM_SRV	*Very Low*	*Low*	1
Networking_HW	*Very Low*	*High*	
Blade_Center	*Very Low*	*High*	6
Misuse of System Resources			
!!Workstation	*Medium*	*High*	6
Networking_HW	*Medium*	*High*	
Blade_Center	*Medium*	*Medium*	5

	Ευπάθεια	Απειλή	Κίνδυνος
Communications Infiltration			
!EMAIL	*Low*	*Medium*	6
!INTRANET	*Very Low*	*Medium*	5
!ERP	*Medium*	*Medium*	6
!BS_STRATEGY	*Medium*	*Medium*	6
!DNS	*Very Low*	*Low*	4
!AUTHENTICATION	*Very Low*	*Low*	4
Communications Failure			
!EMAIL	*Very Low*	*High*	6
!INTRANET	*Low*	*High*	6
!ERP	*Low*	*High*	6
!BS_STRATEGY	*Very Low*	*High*	3
!SMART_CARD	*Very Low*	*High*	3
!BACK_UP	*High*	*High*	2
!DNS	*Very Low*	*High*	4
!AUTHENTICATION	*Very Low*	*High*	5
!USER_FILE	*Very Low*	*High*	6
Networking_HW	*Very Low*	*High*	
Embedding of Malicious Code			
!EMAIL	*High*	*Medium*	7
!INTRANET	*Low*	*Low*	5
Accidental Mis-routing			
!EMAIL	*Very Low*	*Low*	
!INTRANET	*Very Low*	*Low*	3
Technical Failure of Host			
!SMART_CARD_SRV	*Low*	*Low*	3
!BACK_UP_TAPE_SRV	*Medium*	*Low*	1
!BACK_UP_DPM_SRV	*Low*	*Low*	1
Blade_Center	*Medium*	*Medium*	6
Technical Failure of Storage Facility			
Blade_Center	*Medium*	*Medium*	6
Technical Failure of Print Facility			
!!Workstation	*Medium*	*Low*	6

	Ευπάθεια Κίνδυνος	Απειλή	
Technical Failure of Network Distribution Component			
Networking_HW	*Low*	*Medium*	
Technical Failure of Network Gateway			
!ADSL_ROUTER	*Low*	*Medium*	
Power Failure			
!SMART_CARD_SRV	*High*	*Medium*	2
!!Workstation	*High*	*Medium*	6
!BACK_UP_TAPE_SRV	*High*	*Medium*	1
!BACK_UP_DPM_SRV	*High*	*Medium*	1
!ACCOUNTING_DEP_WS	*High*	*Medium*	5
Networking_HW	*High*	*Medium*	
Blade_Center	*High*	*Medium*	6
Air Conditioning Failure			
Networking_HW	*Very Low*	*Medium*	
Blade_Center	*Very Low*	*Medium*	5
System and Network Software Failure			
!SMART_CARD_SRV	*Very Low*	*Medium*	1
!!Workstation	*Very Low*	*Low*	5
!BACK_UP_TAPE_SRV	*Medium*	*High*	
!BACK_UP_DPM_SRV	*Low*	*High*	
Networking_HW	*Low*	*Medium*	
Blade_Center	*Low*	*Medium*	5
Application Software Failure			
!ERP_SW	*Very High*	*High*	5
!BS_STRATEGY_SW	*Very High*	*Low*	5
!SMART_CARD_SW	*Very Low*	*Medium*	1
Hardware Maintenance Error			
!BACK_UP_TAPE_SRV	*Low*	*High*	1
!BACK_UP_DPM_SRV	*Low*	*High*	1
!IBM_STORAGE	*Low*	*High*	5
Blade_Center	*Very Low*	*Medium*	5

	Ευπάθεια	Απειλή	
	Κίνδυνος		
Software Maintenance Error			
!ERP	*Low*	*High*	5
!BS_STRATEGY	*Low*	*Medium*	4
!SMART_CARD	*Very Low*	*Medium*	1
User Error			
!ERP_DATA	*Medium*	*Low*	4
!EMAIL-pst_DATA	*Very High*	*High*	
!EMAIL-box_DATA	*Medium*	*Medium*	
TEAM_DATA_FILES	*Medium*	*Medium*	4
Fire			
Networking_HW	*Low*	*High*	2
Blade_Center	*Very Low*	*High*	6
Theft by Insiders			
!!Workstation	*Medium*	*Medium*	6
!!Media	*Medium*	*Medium*	4
TEAM_DATA_FILES	*High*	*Low*	6
Theft by Outsiders			
!Warehouse	*Very Low*	*High*	6
!Reception	*Very Low*	*High*	6
!Customer_Service	*Very Low*	*High*	6
!Commercial_Department	*Low*	*Medium*	6
Wilful Damage by Insiders			
!!Media	*Very Low*	*Low*	2
!ERP_DATA	*Very Low*	*Medium*	5
!EMAIL-pst_DATA	*Low*	*Low*	2
!EMAIL-box_DATA	*Low*	*Low*	5
TEAM_DATA_FILES	*Low*	*Low*	5
Wilful Damage by Outsiders			
!Warehouse	*Very Low*	*High*	6
!Reception	*Very Low*	*High*	6
!Customer_Service	*Very Low*	*High*	6
!Commercial_Department	*Very Low*	*High*	6

4.3 Ανασκόπηση των αποτελεσμάτων

Σύμφωνα με τον παραπάνω πίνακα, είναι ευνόητο πως ορισμένες απειλές ξεχωρίζουν ως προς το κίνδυνο που δημιουργούν. Η βαθμολογία του κινδύνου των απειλών όπως έχει αναφερθεί και προηγουμένως είναι συνυφασμένη με την αξία , την απειλή αλλά και την ευπάθεια, τα οποία έχουν καθοριστεί από τον μελετητή. Στην συγκεκριμένη μελέτη του συστήματος της X Medicals ο κίνδυνος παίρνει τιμές από πολύ χαμηλές έως αρκετά υψηλές και αυτό οφείλεται κυρίως στις τιμές που δόθηκαν κατά το στάδιο της αξιολόγησης των δεδομένων και του λογισμικού. Στα σημεία όπου δεν έχει γίνει η βαθμολόγηση του κινδύνου από την CRAMM , δεν υπάρχει και κάποιος ουσιαστικός κίνδυνος , άξιος προς μελέτη και ανάλυση. Τα σημεία λοιπόν που έχουν υψηλή βαθμολογία (6 και 7) είναι αυτά που χρειάζονται ιδιαίτερη προσοχή και παραθέτονται στη συνέχεια.

- Μεταμφίεση ταυτότητας χρήστη από Υπόχρεα Πρόσωπα, από συμβεβλημένους πάροχους υπηρεσιών και από τρίτους

Masquerading of User Identity by Insiders
INTRANET , USER_FILE , USER_DATA, INTRANET_DATA, BS_DATA , TEAM_DATA_FILES

- Μη εξουσιοδοτημένη χρήση Εφαρμογής

Unauthorized Use of an Application
ERP

- Εισαγωγή Επιζήμιου ή κακόβουλου Λογισμικού

Introduction of Damaging or Disruptive Software
Workstation

- Κατάχρηση των πόρων του συστήματος

Misuse of System Resources
Workstation

- Διείσδυση Επικοινωνιών - Αποτυχία Επικοινωνιών

Communications	
Infiltration	**Failure**
EMAIL ,ERP ,BS_STRATEGY	EMAIL ,INTRANET ,ERP , USER_FILE

- Ενσωμάτωση του κακόβουλου κώδικα

Embedding of Malicious Code
EMAIL

- Τεχνική βλάβη Εξυπηρετητή, Μέσου αποθήκευσης και Μέσου εκτύπωσης

Technical Failure of		
Host	**Storage Facility**	**Print Facility**
Blade_Center	Blade_Center	Workstation

- Διακοπή ρεύματος

Power Failure
Workstation , Blade_Center

- Φωτιά

Fire
Blade_Center

- Κλοπή από Υπόχρεα Πρόσωπα και από τρίτους

Theft by	
Insiders	**Outsiders**
Workstation , TEAM_DATA_FILES	Warehouse ,Reception, Customer_Service, Commercial_Department

- Θελημένη Ζημιά από Υπόχρεα Πρόσωπα και από τρίτους

Wilful Damage by
Outsiders
Warehouse ,Reception, Customer_Service, Commercial_Department

Οι παραπάνω απειλές είναι αυτές που έχουν την μεγαλύτερη βαρύτητα, για την αντιμετώπιση τους, γιατί έχουν το μεγαλύτερο αντίκτυπο στην συγκεκριμένη μελέτη. Αυτό δεν σημαίνει όμως ότι οι υπόλοιπες απειλές δεν πρέπει να λαμβάνονται υπόψη. Αντιθέτως, όλες οι απειλές πρέπει να αντιμετωπίζονται η κάθε μια ανάλογα με την βαρύτητα της.

<u>Σημείωση</u>

Ο βαθμός του κινδύνου δείχνει ποια περιουσιακά στοιχεία είναι ποιο ευαίσθητα και πρέπει να προστατευτούν αλλά δεν υπολογίζει τα αντίμετρα που ενδεχομένως ήδη υπάρχουν εγκατεστημένα. Δηλαδή μπορεί κάτι να έχει υψηλό βαθμό κινδύνου αλλά να αντιμετωπίζεται ικανοποιητικά από τα υπάρχοντα μέτρα προστασίας.

5 Αντίμετρα (Countermeasure of Risks)

Ο υπολογισμός των αντίμετρων είναι και το τελικό στάδιο της CRAMM. Έχοντας υλοποιήσει την αναγνώριση και αξιολόγηση της όλη συλλογής των πληροφοριών που κρίθηκαν απαραίτητες (αρχικό στάδιο) , έχοντας προσδιορίσει το πλήθος και την κρισιμότητα των απειλών που μπορεί να έχουν στο σύστημα (δεύτερο στάδιο) , πλέον γίνεται εφικτό το τρίτο και τελικό στάδιο της μελέτης , δηλαδή τον προσδιορισμό της αντιμετώπισης των κινδύνων που υπάρχουν στο σύστημα καθώς και τις βελτιώσεις που μπορούν να πάρουν τα ήδη υπάρχοντα μέτρα ελέγχου.

5.1 Μεθοδολογία

Η μεθοδολογία της CRAMM στηρίζεται σε μια μεγάλη βάση δεδομένων κάθε τύπου αντίμετρων (αντίμετρα που προστατεύουν, αντίμετρα που ανιχνεύουν, αντίμετρα που μειώνουν το αντίκτυπο κτλ) , με σκοπό την καλύτερη διασφάλιση της αντιμετώπισης όλων των απειλών. Επειδή αυτά τα αντίμετρα έχουν διαφορετική αποτελεσματικότητα και κόστος υλοποίησης μεταξύ τους, πρέπει να γίνει μια επιλογή των κατάλληλων αντιμέτρων για κάθε περίπτωση. Αυτό γίνεται λαμβάνοντας υπόψη τον τύπο του κάθε περιουσιακού στοιχείου, τις απειλές προς αυτό και τον βαθμό κινδύνου που έχει. Ο τύπος και οι απειλές είναι που καθορίζουν τον τύπο των αντιμέτρων, ενώ ο βαθμός κινδύνου καθορίζει το κόστος υλοποίησης τους. Δηλαδή ένας υψηλός βαθμός κινδύνου δικαιολογεί και αντίμετρα με υψηλό κόστος υλοποίησης.

Η υλοποίηση της μεθοδολογίας που αναφέρθηκε , δηλαδή ο υπολογισμός των αντιμέτρων, είναι μια χρονοβόρα και όχι απλή διαδικασία και αυτό διότι τα αντίμετρα, πέρα από το πλήθος τους , δεν προστατεύουν από μια μόνο απειλή αλλά από διάφορες , από τις οποίες μερικές μπορεί να αλληλεπικαλύπτονται.

Στη συνέχεια αυτής της μελέτης παρουσιάζονται τα αντίμετρα που υπολογίστηκαν από την CRAMM για την X Medicals.

5.2 Αντίμετρα του συστήματος της X Medicals

Τα αντίμετρα που παράχθηκαν από την CRAMM για την ανάλυση των κινδύνων της εταιρίας X Medicals παραθέτονται παρακάτω χωρισμένα ανά κατηγορίες , με σκοπό την καλύτερη διαχείριση τους.

Accommodation Moves
Accounting
Anti-spamming controls
Application Input/Output Controls
Audit
Back-up of Data
Business Continuity Planning
Capacity Planning
Compliance Checks
Content Scanning
Data Protection Legislation
Document / Media Controls
Equipment Failure Protection
Fire Protection
Identification and Authentication
Incident Handling
Insurance
Logical Access Control
Mobile Computing and Teleworking
Network Access Controls
Network Security Management
Object Re-use
Personnel
Physical Equipment Protection
Power Protection
Protection Against Malicious Software
Recovery Option for Hosts
Recovery Options for Accommodation
Security Education and Training
Security Infrastructure
Security Policy
Security Testing
Site / Building Physical Security
Software Distribution
Software Integrity
System Administration Controls
System Input/Output Controls
Theft Protection
Vulnerability Analysis
Physical Equipment Protection
Power Protection
Protection Against Malicious Software
Recovery Option for Hosts
Recovery Options for Accommodation
Security Education and Training
Security Infrastructure

Τα παραπάνω αντίμετρα που επιλέχθηκαν από την CRAMM είναι αποτέλεσμα μέσα από τις πληροφορίες που έχει αποδώσει η μελέτη πάνω στην εταιρία X Medicals. Συνεπώς όλα αυτά μπορούν να κριθούν και ως ενδεικτικά , διότι δεν είναι απαραίτητη η υλοποίησή τους. Κάποια μπορεί να είναι μη εφαρμόσιμα λόγω κάποιων ιδιαιτεροτήτων του πληροφοριακού συστήματος , κάποια να κριθούν ακριβά για το σκοπό τους , όλα δηλαδή, θα φιλτραριστούν από τον ανθρώπινο παράγοντα , τον υπεύθυνο του έργου, που γνωρίζει καλύτερα την λειτουργία του όλου συστήματος. Παρόλα αυτά η CRAMM "οφείλει" να παρουσιάσει όλα τα αντίμετρα , έτσι ώστε αν είναι επιθυμητή η πλήρης κάλυψη των απειλών που υπάρχουν, να υπάρχει η δυνατότητα να επιλεχθούν αντίμετρα από όλες τις κατηγορίες.

5.3 Εκτίμηση αναγκών ασφαλείας – X Medicals

Έχοντας ολοκληρώσει και το τελευταίο στάδιο της CRAMM , είναι εφικτή πλέον η εκτίμηση και των αναγκών ασφαλείας του πληροφοριακού συστήματος της X Medicals. Η συλλογή όλων αυτών των πληροφοριών δίνει την δυνατότητα της εστίασης στα πιο σημαντικά προβλήματα ασφαλείας στο παρόν πληροφοριακό σύστημα. Παρακάτω παρουσιάζονται τα σημαντικότερα προβλήματα - κενά ασφαλείας καθώς και οι προτάσεις αντιμετώπισής τους.

Identification and Authentication

Ένα μεγάλο και σημαντικό κομμάτι της ασφάλειας σε ένα πληροφοριακό σύστημα είναι ο τομέας της αναγνώρισης και πιστοποίησης. Όταν μέσα σε ένα σύστημα υπάρχουν διαφορετικού τύπου δεδομένα και εφαρμογές , θα πρέπει να υπάρχει και η ανάλογη ευελιξία για την ασφάλειά τους. Συγκεκριμένα , στο κομμάτι αυτό υπάρχουν αρκετά κενά σημεία στην εφαρμογή BS Strategy. Αυτή η εφαρμογή, όπως έχει αναφερθεί και στο μέρος της αναγνώρισης των περιουσιακών στοιχείων, είναι ένα εργαλείο αναφορών - εκτυπώσεων, που χρησιμοποιεί κυρίως το εμπορικό τμήμα της εταιρίας αλλά και η διοίκηση. Δεν είναι εφικτή μέσω αυτού η τροποποίηση των δεδομένων , παρά μόνο η συλλογή – εμφάνιση των δεδομένων. Η ασφάλεια αυτών των δεδομένων ως προς τη διαγραφή ή τη μετατροπή τους βρίσκεται σε ικανοποιητικά επίπεδα, όμως ως προς την υποκλοπή τους εμφανίζει κενά. Σε αυτή την εφαρμογή δεν υπάρχουν ξεχωριστοί λογαριασμοί για τον κάθε χρήστη , παρά μόνο κάποια group χρηστών. Συνεπώς ο κωδικός των ομάδων αυτών δεν είναι τόσο ασφαλής , καθώς διαμοιράζεται από αρκετούς χρήστες. Ο κωδικός αυτός δεν έχει κάποια αυστηρή πολιτική ούτε για το μέγεθός του , αλλά ούτε και για την πολυπλοκότητά του με αποτέλεσμα να χρησιμοποιούνται κωδικοί μικροί και απλοί . Επιπλέον η εφαρμογή έχει τη δική της φόρμα εισόδου (login screen) χωρίς να απαιτεί για το άνοιγμά της κάποια επιπλέον ασφάλεια (πχ αυθεντικοποίηση χρήστη του τομέα - domain user).

Σύμφωνα με όλα τα παραπάνω είναι αντιληπτό πως η εφαρμογή BS Strategy της X Medicals παρουσιάζει μια μεγάλη ευαισθησία στην περίπτωση της υποκλοπής των δεδομένων , περισσότερο στις περιπτώσεις όπου η υποκλοπή γίνεται από μέσα και λιγότερο από τρίτο πρόσωπο. Η εταιρία είναι φανερό πως δεν έχει δώσει μεγάλη σημασία για τους κινδύνους που μπορούν να προκύψουν από αυτά τα κενά ασφαλείας. Ένα άμεσο μέτρο αντιμετώπισης είναι να χρησιμοποιηθεί μια πιο αυστηρή πολιτική για τους κωδικούς εισαγωγής, καθώς οι χρήστες να μετατραπούν σε ατομικό επίπεδο από ομαδικό. Κάθε ένας δηλαδή να έχει τον προσωπικό του κωδικό ώστε και η καταγραφή των κινήσεων να γίνεται ανά χρήστη και όχι ανά ομάδα, με πιθανό αποτέλεσμα να κάνει τους χρήστες και πιο επιφυλακτικούς.

Ένα παρόμοιο φαινόμενο με την προηγούμενη εφαρμογή διαπιστώθηκε και στην εφαρμογή του ERP της εταιρίας. Δεν υπάρχει κάποια αυστηρή πολιτική στο θέμα του κωδικού εισαγωγής (Log on screen). Ο μόνος περιορισμός, είναι ο κωδικός να μην είναι μικρότερος από τέσσερα ψηφία, πράγμα που το καθιστά αρκετά ευάλωτο. Ένα άλλο κενό του ERP είναι πως κατά το άνοιγμα της εφαρμογής , στη φόρμα εισαγωγής κωδικού, εμφανίζονται κάποια στοιχεία (ονόματα βάσεων δεδομένων) , τα οποία θα μπορούσε να τα εκμεταλλευτεί κάποιος επίδοξος κακόβουλος χρήστης. Ένα άμεσο μέτρο ασφαλείας είναι είτε η αφαίρεση των στοιχείων αυτών, από τη πρώτη φόρμα, είτε η κωδικοποίηση τους σε τίτλους που δεν έχουν κάποια σχέση με το πραγματικό

τους όνομα και όσο αναφορά τον κωδικό , να γίνει αλλαγή τους με πιο αυστηρούς περιορισμούς καθώς και η υποχρεωτική περιοδική αλλαγή ανά εξάμηνο ή και τρίμηνο.

Security Policy (Physical Equipment Protection)

Οι πολιτικές ασφαλείας που εφαρμόζονται στην εταιρία X Medicals βρίσκονται σε ικανοποιητικά και εφησυχαστικά επίπεδα σύμφωνα με τα αποτελέσματα της CRAMM. Από θέμα πληρότητας και ευρύτητας αυτών των πολιτικών η εταιρία είναι σε σωστά πλαίσια, το μόνο που χρειάζεται προσοχή είναι και η εφαρμογή αυτών , και μάλιστα η αυστηρή εφαρμογή σε περιπτώσεις που είναι μείζων σημασίας. Το σημείο που είναι άξιο αναφοράς σε αυτό το κομμάτι της ασφάλειας είναι πάνω στο θέμα των Tape Back up. Ενώ γίνεται το back up με αυστηρό προγραμματισμό και έλεγχο , δεν εφαρμόζεται όμως η μετακίνηση των κασετών (Tapes) σε χώρο ασφαλή και εκτός αυτού που βρίσκεται και ο Tape Back up Server. Αυτό το μέτρο προφύλαξης είναι σε περίπτωση που στον χώρο προκληθεί κάποια καταστροφή να μην καταστραφούν και τα back up δεδομένα.

Security Testing

Ένα σημαντικό σημείο που φαίνεται να υπάρχουν μεγάλα κενά στην X Medicals είναι οι έλεγχοι πάνω στα συστήματα ασφαλείας. Πέρα από τα δεδομένα (data) στα οποία υπάρχει ένας υποτυπώδες έλεγχος , δεν υπάρχει κάποια άλλη μέθοδος ελέγχου στα συστήματα ασφαλείας. Ενώ υπάρχουν αρκετά μέτρα ασφαλείας στο πληροφοριακό σύστημα , δεν υπάρχει μια διαδικασία για τον έλεγχο αυτών και κατά πόσο μπορούν να παρακαμφτούν. Θα πρέπει να υπάρχει ένα συνολικό πλάνο ελέγχου όλων των συστημάτων ασφαλείας το οποίο θα πρέπει να εκτελείται ανά τακτά χρονικά διαστήματα. Επίσης θα πρέπει να υπάρχουν και επιμέρους , πιο συγκεκριμένες διαδικασίες ελέγχου για τον έλεγχο των πιο καίριων σημείων της εταιρίας είτε του πληροφοριακού συστήματος είτε φυσικών αγαθών.

Mobile Computing and Teleworking

Μια από τις φυσικές τοποθεσίες που δεν περιλαμβάνονται στον έλεγχο ασφαλείας smart card και είναι άμεσα προσβάσιμη και από τρίτο πρόσωπο , είναι το εμπορικό τμήμα (commercial department). Σε αυτό βρίσκονται φορητές συσκευές τύπου laptop , projectors και αρκετά έγγραφα. Όλα αυτά δεν προστατεύονται με κάποιο τρόπο και αφήνεται πάνω στον χρήστη που τα έχει υπό ευθύνη του. Το γεγονός πως το εμπορικό τμήμα έχει μόνο φορητές συσκευές , είναι για ευνόητους λόγους κατανοητό , αλλά στην περίπτωση που οι συσκευές και τα έγγραφα μένουν στο τμήμα , θα πρέπει να υπάρχει μια ασφαλή τοποθεσία για την προφύλαξή τους. Ενώ το τμήμα διαθέτει ασφαλείς χώρους, δεν χρησιμοποιούνται, με αποτέλεσμα να μένουν εκτεθειμένα. Θα πρέπει σε αυτό το κομμάτι της ασφάλειας να υπάρχει ένας έλεγχος για το τι μένει εκτεθειμένο , και κάποιες συγκεκριμένες διαδικασίες για την αντιμετώπιση τέτοιων θεμάτων.

Άλλο ένα τέτοιο θέμα είναι και η προστασία των PDA στην αποθήκη. Ενώ τα PDA είναι χρεωμένα σε συγκεκριμένα πρόσωπα που τα χειρίζονται και ανήκουν στο τμήμα της αποθήκης μένουν και αυτά εκτεθειμένα στις περιπτώσεις που δεν χρησιμοποιούνται. Στην αποθήκη έχουν συγκεκριμένα πρόσωπα πρόσβαση χωρίς όμως αυτά να έχουν και πρόσβαση στα PDA. Για αυτό το λόγο θα πρέπει τα PDA όταν είναι ανενεργά να μένουν και προστατευμένα από το υπόλοιπο προσωπικό που έχει πρόσβαση στην αποθήκη.

Business Continuity Planning

Ο σχεδιασμός του πληροφοριακού συστήματος αλλά και ένα μεγάλο μέρος των κύριων διαδικασιών της εταιρίας ως προς τη συνοχή και τη συνέχεια που πρέπει να παρουσιάζει είναι αρκετά ικανοποιητικός αλλά με μερικά κενά. Ένα από τα σημαντικότερα κενά που φαίνεται να υπάρχει είναι η παραγωγή των δοκιμών σε συνθήκες καταστροφής (IT system failure test). Ενώ οι λύσεις υπάρχουν και έχουν δοκιμαστεί υπό κανονικές συνθήκες , δεν υπάρχουν κάποια προσχεδιασμένα πλάνα καταστροφής , αλλά και οι δοκιμές αυτών. Επίσης για τα προσωπικά δεδομένα user data και email-pst υπάρχουν κάποιες διαδικασίες που έχουν δημιουργηθεί σε περιπτώσεις μερικής ή ολικής καταστροφής αλλά επαφίενται στον κάθε χρήστη ξεχωριστά. Κάθε χρήστης δηλαδή είναι υπεύθυνος για την εκτέλεση των διαδικασιών που υπάρχουν για τα συγκεκριμένα αρχεία. Το σημαντικότερο που πρέπει να γίνει σε αυτήν την περίπτωση , είναι η παραγωγή ενός προγράμματος δοκιμών για το λεγόμενο crisis management. Αυτό το πρόγραμμα θα πρέπει να περιέχει διαφορετικών τύπου δοκιμές , τεχνικά , κανονικά , μικρά και ολοκληρωμένα test.

Theft Protection

Σύμφωνα με τα αποτελέσματα της CRAMM στο τομέα της κλοπής και συγκεκριμένα από πρόσωπα εντός της εταιρίας , υπάρχουν αρκετά κενά ασφαλείας. Τα περισσότερα από αυτά είναι κυρίως διαδικασίες ή αλλιώς μέτρα διασφάλισης για αγαθά που χωρίς κάποια άδεια δεν θα έπρεπε να βγαίνουν εκτός εταιρίας. Δεν υπάρχει κανένας έλεγχος τέτοιου τύπου καθώς δεν έχουν αναφερθεί τέτοια περιστατικά. Βέβαια το ότι δεν έχουν αναφερθεί περιστατικά κλοπής δεν σημαίνει πως δεν έχουν γίνει και πως απλά αγνοούνται. Κάποια πιθανά μέτρα αντιμετώπισης είναι να δημιουργούνται γραπτές και όχι προφορικές οι άδειες για την κατοχή και μετακίνηση αγαθών εκτός εταιρίας , να υπάρχουν συχνοί έλεγχοι κατά την έξοδο , όπως επίσης ενημέρωση κατά την είσοδο αγαθού που δεν ανήκει στην εταιρία.

Security Infrastructure

Γενικότερα στην υποδομή της ασφάλειας της εταιρίας παρατηρήθηκαν κενά στην απόδοση ευθυνών κυρίως για τα φυσικά αγαθά. Ενώ υπάρχει ιεραρχική δομή για λειτουργίες και διαδικασίες που χρειάζονται για την υλοποίηση της ροής της εργασίας δεν υπάρχουν ευθύνες για συγκεκριμένες διαδικασίες ασφαλείας που να καθορίζονται ρητά και που να τεκμηριώνονται. Το τμήμα του ανθρώπινου δυναμικού θα πρέπει να είναι αυτό που θα καθορίσει τις διαδικασίες αυτές , όπως επίσης και συγκεκριμένες ομάδες / υπαλλήλους , που θα είναι υπεύθυνοι σε συγκεκριμένους τομείς / τμήματα.

6 ΕΠΙΛΟΓΟΣ - Σύνοψη Μελέτης

Η διαδικασία ανάλυσης και μελέτης της ασφάλειας ενός πληροφοριακού συστήματος ή έστω ενός τμήματος αυτού , απαιτεί μεγάλη προσοχή και σοβαρότητα. Κάθε στάδιο της έχει και την ανάλογη βαρύτητα για την πρόοδο του όλου έργου. Η συγκέντρωση – συλλογή όλων των πληροφοριών που συσχετίζονται με τη μελέτη , η ανάλυση αυτών για την πλήρη κατανόηση των εξεταζόμενων λειτουργιών και η προσεχτική επεξεργασία των αποτελεσμάτων , είναι τα βασικά στάδια που πρέπει να ακολουθηθούν , ώστε οι τελικές αποφάσεις που θα παρθούν να είναι και οι καλύτερες δυνατές επιλογές για την ασφάλεια ενός πληροφοριακού συστήματος.

Η συγκεκριμένη μελέτη , χρησιμοποιώντας την εφαρμογή CRAMM και ακλουθώντας αυστηρά τα βήματα και τη μεθοδολογία της , συνάντησε ένα πληροφοριακό σύστημα φτιαγμένο με υψηλές προδιαγραφές τεχνολογίας , αυτοματοποίησης αλλά και συνοχής. Η ασφάλεια αυτού μπορεί να χαρακτηριστεί αρκετά ικανοποιητική αλλά με μερικά σημαντικά κενά και κάποια περιθώρια βελτίωσης. Τα περισσότερα κενά οφείλονται στην εμπιστοσύνη που δείχνει η πολιτική της εταιρίας απέναντι στους υπαλλήλους της. Ενώ, δηλαδή , υπάρχουν κατά ένα μεγάλο ποσοστό, οι σωστά δομημένες διαδικασίες και ο σύγχρονος τεχνολογικός εξοπλισμός για την πληρότητα της ασφάλειας που απαιτείται , δεν υπάρχει η σωστή και αυστηρή μεθοδικότητα που πρέπει να ακολουθηθεί . Το σημαντικότερο κενό που παρουσιάζεται είναι η μη ύπαρξη των κατάλληλων πλάνων και συνεχών δοκιμών, όπου θα γίνεται ο έλεγχος της ασφάλειας όλου του πληροφοριακού συστήματος αλλά και των μεμονωμένων στοιχείων του.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] CRAMM Version 5.1 User Guide

[2] Ρεκλέτης Ε. , Πρακτικός οδηγός του εργαλείου ασφάλειας CRAMM , Πειραιάς

[3] Νικήτα Γ. ,2004,Ανάλυση Κινδύνων Πληροφοριακών Συστημάτων, Θεσσαλονίκη

[4] www.InfoSecurityAnalysis.com

[5] Siemens insight Consulting, Business continuity management "Planning for the Unexpected",

United Kingdom

[6] Siemens insight Consulting, "Crisis Management" , United Kingdom

[7] Siemens Insight Consulting,11 October 2005, "The Logic behind CRAMM'sAssessment of

Measures of Risk and Determination of Appropriate Countermeasures" , United Kingdom

[8] Siemens Insight Consulting,17 October 2005, "Integrating Security into IT Projects and

Programmes" , United Kingdom

[9] Siemens Insight Consulting, "Legal and Regulatory Compliance" , United Kingdom

[10] Vijay Gawde , Information Systems Misuse - Threats & Countermeasures

[11] Ι.Ζαμπετάκη, Χ.Ροζάκη, 17 Δεκεμβρίου 2009 ,Enterprise IT Security Conference "Αλλάξτε τρόπο σκέψης" ,Αθήνα ,www.netweek.gr/

ΠΑΡΑΡΤΗΜΑ Α

Αναλυτική αξιολόγηση πληροφοριακού συστήματος X Medicals

Αξιολόγηση Δεδομένων , Φυσικών αγαθών και αγαθών Λογισμικού.

Data Asset Valuation

Data Asset	AUTHENTICATION_DATA
Type of Data	Safety Related
Interviewees	Patousakis George
Interviewers	Chlis Kalogeropoulos Elias
Date	
Status	

Description of Data

Impacts

Unavailability - less than 15 minutes	Guideline	Scale Value	Financial Value
	Policy and Operations of Public Servi	1	
Unavailability - 3 hours	Guideline	Scale Value	Financial Value
	Policy and Operations of Public Servi	5	
Unavailability - 1 day	Guideline	Scale Value	Financial Value
	Financial Loss	4	
Unavailability - 2 days	Guideline	Scale Value	Financial Value
	Financial Loss	8	
Destruction since the last successful back-up	Guideline	Scale Value	Financial Value
	Financial Loss	9	
Total destruction including back-ups	Guideline	Scale Value	Financial Value
	Disruption to Activities	10	

Data Asset Valuation

Data Asset AUTHENTICATION_DATA

Unauthorised disclosure to insiders	Guideline	Scale Value	Financial Value
	Security and Intelligence	8	

Unauthorised disclosure to outsiders	Guideline	Scale Value	Financial Value
	Commercial and Economic Interests	8	

Deliberate modification	Guideline	Scale Value	Financial Value
	Disruption to Activities	7	

Data Asset Valuation

Data Asset	BACK_UP_DATA
Type of Data	Safety Related
Interviewees	Patousakis George
Interviewers	Chlis Kalogeropoulos Elias
Date	
Status	

Description of Data

Impacts

Unavailability - 1 day	Guideline	Scale Value	Financial Value
	Management and Business Operations	1	
Unavailability - 1 week	Guideline	Scale Value	Financial Value
	Management and Business Operations	8	
Unavailability - 2 weeks	Guideline	Scale Value	Financial Value
	Management and Business Operations	10	

Data Asset Valuation

Data Asset	BS_DATA
Type of Data	Commercially Sensitive
Interviewees	Patousakis George, Vakchos Kostas
Interviewers	Chlis Kalogeropoulos Elias
Date	
Status	

Description of Data

Impacts

Unavailability - 3 hours	Guideline	Scale Value	Financial Value
	Disruption to Activities	2	
Unavailability - 1 day	Guideline	Scale Value	Financial Value
	Management and Business Operations	4	
Unavailability - 1 week	Guideline	Scale Value	Financial Value
	Management and Business Operations	10	
Destruction since the last successful back-up	Guideline	Scale Value	Financial Value
	Management and Business Operations	8	
Total destruction including back-ups	Guideline	Scale Value	Financial Value
	Management and Business Operations	10	
Unauthorised disclosure to outsiders	Guideline	Scale Value	Financial Value
	Commercial and Economic Interests	9	

Data Asset Valuation

Data Asset	BS_DATA

Deliberate modification	Guideline	Scale Value	Financial Value
	Management and Business Operations	9	

Data Asset Valuation

Data Asset	COMMON-FILES_DATA
Type of Data	Commercially Sensitive
Interviewees	Patousakis George, Vakchos Kostas, Zafos George
Interviewers	Chlis Kalogeropoulos Elias
Date	
Status	

Description of Data

Impacts

Unavailability - 1 hour	Guideline	Scale Value	Financial Value
	Disruption to Activities	8	
Unavailability - 3 hours	Guideline	Scale Value	Financial Value
	Disruption to Activities	10	
Unavailability - 1 day	Guideline	Scale Value	Financial Value
	Financial Loss	5	
Unavailability - 2 days	Guideline	Scale Value	Financial Value
	Financial Loss	8	
Unavailability - 1 week	Guideline	Scale Value	Financial Value
	Management and Business Operations	5	

Data Asset Valuation

Data Asset	CRITICAL-FILES_DATA
Type of Data	Financial
Interviewees	Patousakis George, Vakchos Kostas
Interviewers	Chlis Kalogeropoulos Elias
Date	
Status	

Description of Data

Impacts

Unavailability - 1 hour	Guideline	Scale Value	Financial Value
	Commercial and Economic Interests	3	
Unavailability - 3 hours	Guideline	Scale Value	Financial Value
	Disruption to Activities	3	
Unavailability - 1 day	Guideline	Scale Value	Financial Value
	Management and Business Operations	2	
Unavailability - 2 days	Guideline	Scale Value	Financial Value
	Management and Business Operations	5	

Data Asset Valuation

Data Asset	DNS_DATA
Type of Data	Other Data Types
Interviewees	Patousakis George
Interviewers	Chlis Kalogeropoulos Elias
Date	
Status	

Description of Data

Impacts

Unavailability - 1 hour	Guideline	Scale Value	Financial Value
	Policy and Operations of Public Servi	5	
Unavailability - 3 hours	Guideline	Scale Value	Financial Value
	Financial Loss	3	
Unavailability - 1 day	Guideline	Scale Value	Financial Value
	Financial Loss	7	
Destruction since the last successful back-up	Guideline	Scale Value	Financial Value
	Disruption to Activities	8	
Total destruction including back-ups	Guideline	Scale Value	Financial Value
	Disruption to Activities	10	
Unauthorised disclosure to outsiders	Guideline	Scale Value	Financial Value
	Security and Intelligence	4	

Data Asset Valuation

Data Asset	DNS_DATA

Deliberate modification	Guideline	Scale Value	Financial Value
	Disruption to Activities	7	

Data Asset Valuation

Data Asset	EMAIL-box_DATA
Type of Data	Commercially Sensitive
Interviewees	Patousakis George, Vakchos Kostas
Interviewers	Chlis Kalogeropoulos Elias
Date	
Status	

Description of Data

Impacts

Unavailability - 1 hour	Guideline	Scale Value	Financial Value
	Disruption to Activities	5	
Unavailability - 3 hours	Guideline	Scale Value	Financial Value
	Disruption to Activities	7	
Unavailability - 1 day	Guideline	Scale Value	Financial Value
	Disruption to Activities	10	
Unavailability - 2 days	Guideline	Scale Value	Financial Value
	Loss of Goodwill	7	
Unavailability - 1 week	Guideline	Scale Value	Financial Value
	Policy and Operations of Public Servi	5	

Data Asset Valuation

Data Asset	EMAIL-pst_DATA
Type of Data	Personal
Interviewees	Patousakis George
Interviewers	Chlis Kalogeropoulos Elias
Date	
Status	

Description of Data

Impacts

Unavailability - 1 hour	Guideline	Scale Value	Financial Value
	Disruption to Activities	1	
Unavailability - 3 hours	Guideline	Scale Value	Financial Value
	Disruption to Activities	2	
Unavailability - 1 day	Guideline	Scale Value	Financial Value
	Disruption to Activities	4	
Unavailability - 1 week	Guideline	Scale Value	Financial Value
	Disruption to Activities	8	

Data Asset Valuation

Data Asset	ERP_DATA
Type of Data	Financial
Interviewees	Patousakis George, Vakchos Kostas, Zafos George
Interviewers	Chlis Kalogeropoulos Elias
Date	
Status	

Description of Data

Impacts

Unavailability - less than 15 minutes	Guideline	Scale Value	Financial Value
	Disruption to Activities	2	
Unavailability - 1 hour	Guideline	Scale Value	Financial Value
	Disruption to Activities	6	
Unavailability - 12 hours	Guideline	Scale Value	Financial Value
	Policy and Operations of Public Servi	9	
Unavailability - 1 day	Guideline	Scale Value	Financial Value
	Financial Loss	8	
Unavailability - 1 week	Guideline	Scale Value	Financial Value
	Financial Loss	10	
Destruction since the last successful back-up	Guideline	Scale Value	Financial Value
	Law Enforcement	8	

Data Asset Valuation

Data Asset ERP_DATA

	Guideline	Scale Value	Financial Value
Total destruction including back-ups	Law Enforcement	10	
Unauthorised disclosure to outsiders	Commercial and Economic Interests	8	
Deliberate modification	Law Enforcement	8	
Insertion of false messages	Financial Loss	8	

Data Asset Valuation

Data Asset	INTRANET_DATA
Type of Data	Commercially Sensitive
Interviewees	Patousakis George, Vakchos Kostas, Zafos George
Interviewers	Chlis Kalogeropoulos Elias
Date	
Status	

Description of Data

Impacts

Unavailability - 1 hour	Guideline	Scale Value	Financial Value
	Disruption to Activities	4	
Unavailability - 3 hours	Guideline	Scale Value	Financial Value
	Disruption to Activities	7	
Unavailability - 1 day	Guideline	Scale Value	Financial Value
	Disruption to Activities	9	
Unavailability - 2 days	Guideline	Scale Value	Financial Value
	Management and Business Operations	10	
Unavailability - 2 months and over	Guideline	Scale Value	Financial Value
	Financial Loss	4	
Destruction since the last successful back-up	Guideline	Scale Value	Financial Value
	Disruption to Activities	8	

Data Asset Valuation

Data Asset INTRANET_DATA

	Guideline	Scale Value	Financial Value
Total destruction including back-ups	Disruption to Activities	10	
Unauthorised disclosure to outsiders	Commercial and Economic Interests	6	
Deliberate modification	Loss of Goodwill	8	

Data Asset Valuation

Data Asset	SMART_CARD_DATA
Type of Data	Safety Related
Interviewees	Patousakis George, Vakchos Kostas
Interviewers	Chlis Kalogeropoulos Elias
Date	
Status	

Description of Data

Impacts

Unavailability - 1 hour	Guideline Security and Intelligence	Scale Value 2	Financial Value
Unavailability - 3 hours	Guideline Disruption to Activities	Scale Value 2	Financial Value
Unavailability - 1 day	Guideline Security and Intelligence	Scale Value 5	Financial Value
Unavailability - 2 days	Guideline Disruption to Activities	Scale Value 5	Financial Value
Unavailability - 1 week	Guideline Financial Loss	Scale Value 6	Financial Value

Data Asset Valuation

Data Asset	USER_DATA
Type of Data	Personal
Interviewees	Patousakis George, Zafos George
Interviewers	Chlis Kalogeropoulos Elias
Date	
Status	

Description of Data

Impacts

Unavailability - 1 hour	Guideline	Scale Value	Financial Value
	Disruption to Activities	2	
Unavailability - 3 hours	Guideline	Scale Value	Financial Value
	Disruption to Activities	4	
Unavailability - 1 day	Guideline	Scale Value	Financial Value
	Disruption to Activities	7	
Unavailability - 2 days	Guideline	Scale Value	Financial Value
	Disruption to Activities	10	
Destruction since the last successful back-up	Guideline	Scale Value	Financial Value
	Disruption to Activities	8	
Total destruction including back-ups	Guideline	Scale Value	Financial Value
	Disruption to Activities	10	

Data Asset Valuation

Data Asset USER_DATA

Unauthorised disclosure to outsiders	Guideline	Scale Value	Financial Value
	Commercial and Economic Interests	8	

Deliberate modification	Guideline	Scale Value	Financial Value
	Disruption to Activities	7	

END OF REPORT

Physical Asset	Number	Scale	Replacement Cost
ACCOUNTING_DEP_WS	2	2	3.600 €
Class: Workstation, Other Workstation; Print Facilities, Printer			
Notes:			
ADSL_ROUTER	1	2	4.000 €
Class: Network Distribution Component, Router; Network Distribution Component, Modem			
Notes:			
APP_SRV	1	2	5.000 €
Class: Host, Application Server			
Notes:			
BACK_UP_DPM_SRV	1	2	3.200 €
Class: Host, Other Host; Storage Device, Other Storage Device			
Notes:			
BACK_UP_TAPE_SRV	1	2	3.000 €
Class: Host, Other Host; Storage Device, Magnetic Tape Device			
Notes:			
COMMERCIAL_DEP_WS	3	3	12.000 €
Class: Workstation, Other Workstation; Workstation, Portable; Print Facilities, Printer			
Notes:			
CUST_SERV_WS	3	2	1.800 €
Class: Workstation, Other Workstation; Print Facilities, Printer; Peripheral Devices, Fax Machines			
Notes:			

Physical Asset	Number	Scale	Replacement Cost
DC_SRV	2	2	4.600 €
Class: Host, General Purpose Network Host			
Notes:			
ERP_SRV	1	2	5.000 €
Class: Host, Database Server			
Notes:			
EXCH_SRV	1	2	5.800 €
Class: Host, Other Host			
Notes:			
FILE_SRV	1	2	3.000 €
Class: Host, File Server			
Notes:			
IBM_STORAGE	1	2	3.500 €
Class: Storage Device, Other Storage Device			
Notes:			
IT_WS	2	2	3.000 €
Class: Workstation, Portable; Workstation, Other Workstation; Print Facilities, Printer			
Notes:			
MANAGEMENT_WS	2	2	2.800 €
Class: Workstation, Other Workstation; Print Facilities, Printer; Workstation, Portable; Peripheral Devices, Fax Machines			
Notes:			

Physical Asset	Number	Scale	Replacement Cost
RECEPTION_WS	2	2	1,300 €
Class: Print Facilities, Printer; Workstation, Other Workstation			
Notes:			
SC_DEV_ACCOUNTING	1	1	400 €
Class: Media, Electronic, Other Electronic Media			
Notes:			
SC_DEV_COMPUTER_ROOM	1	1	400 €
Class: Media, Electronic, Other Electronic Media			
Notes:			
SC_DEV_ENTRANCE	1	1	400 €
Class: Media, Electronic, Other Electronic Media			
Notes:			
SC_DEV_MANAGEMENT	1	1	400 €
Class: Media, Electronic, Other Electronic Media			
Notes:			
SC_DEV_SERVICE	1	1	400 €
Class: Media, Electronic, Other Electronic Media			
Notes:			
SC_DEV_WAREHOUSE	1	1	400 €
Class: Media, Electronic, Other Electronic Media			
Notes:			

Physical Asset	Number	Scale	Replacement Cost
SERVICE_WS	1	1	1.000 €
Class: Workstation, Portable; Print Facilities, Printer; Workstation, Other Workstation			
Notes:			
SMART_CARD_SRV	1	2	2.500 €
Class: Host, Database Server; Host, Application Server			
Notes:			
SWITCH	3	2	1.800 €
Class: Network Distribution Component, Ethernet/Gigabit Switch			
Notes:			
WAREHOUSE_WS	2	2	4.000 €
Class: Workstation, Personal Digital Assistant (PDA); Print Facilities, Printer; Workstation, Other Workstation			
Notes:			
WEB_SRV	1	2	2.000 €
Class: Host, Other Host			
Notes: INTRANET			
		Total	75.300 €

END OF REPORT

Software Asset Valuation

Software Asset	BS_STRATEGY_SW
Type of Software	Package - Financial
Interviewees	Patousakis George, Vakchos Kostas
Interviewers	Chlis Kalogeropoulos Elias
Date	
Status	

Description of Software

Impacts

Unavailability - 1 hour	Guideline	Scale Value	Financial Value
	Disruption to Activities	3	
Unavailability - 1 day	Guideline	Scale Value	Financial Value
	Management and Business Operations	5	
Unavailability - 2 days	Guideline	Scale Value	Financial Value
	Management and Business Operations	10	
Unavailability - 1 week	Guideline	Scale Value	Financial Value
	Disruption to Activities	5	
Destruction since the last successful back-up	Guideline	Scale Value	Financial Value
	Management and Business Operations	6	
Total destruction including back-ups	Guideline	Scale Value	Financial Value
	Management and Business Operations	10	

Software Asset Valuation

Software Asset BS_STRATEGY_SW

Unauthorised disclosure to outsiders	Guideline	Scale Value	Financial Value
	Commercial and Economic Interests	10	

Deliberate modification	Guideline	Scale Value	Financial Value
	Management and Business Operations	5	

Software Asset Valuation

Software Asset	ERP_SW
Type of Software	Bespoke Sensitive - Financial
Interviewees	Patousakis George, Vakchos Kostas, Zafos George
Interviewers	Chlis Kalogeropoulos Elias
Date	
Status	

Description of Software

Impacts

Unavailability - 1 hour	Guideline	Scale Value	Financial Value
	Disruption to Activities	5	
Unavailability - 1 day	Guideline	Scale Value	Financial Value
	Disruption to Activities	9	
Unavailability - 2 days	Guideline	Scale Value	Financial Value
	Financial Loss	10	
Unavailability - 1 week	Guideline	Scale Value	Financial Value
	Legal and Regulatory Obligations	4	
Unavailability - 2 weeks	Guideline	Scale Value	Financial Value
	Legal and Regulatory Obligations	7	
Unavailability - 2 months and over	Guideline	Scale Value	Financial Value
	Legal and Regulatory Obligations	10	

Software Asset Valuation

Software Asset ERP_SW

	Guideline	Scale Value	Financial Value
Destruction since the last successful back-up	Law Enforcement	7	
Total destruction including back-ups	Guideline	Scale Value	Financial Value
	Law Enforcement	10	
Unauthorised disclosure to outsiders	Guideline	Scale Value	Financial Value
	Commercial and Economic Interests	10	
Deliberate modification	Guideline	Scale Value	Financial Value
	Law Enforcement	8	

Software Asset Valuation

Software Asset	SMART_CARD_SW
Type of Software	Package - Safety Critical
Interviewees	Patousakis George, Vakchos Kostas
Interviewers	Chlis Kalogeropoulos Elias
Date	
Status	

Description of Software

Impacts

Unavailability - 1 day	Guideline	Scale Value	Financial Value
	Security and Intelligence	1	
Unavailability - 1 week	Guideline	Scale Value	Financial Value
	Security and Intelligence	5	
Unavailability - 2 weeks	Guideline	Scale Value	Financial Value
	Management and Business Operations	5	
Unavailability - 1 month	Guideline	Scale Value	Financial Value
	Security and Intelligence	10	

END OF REPORT

ΠΑΡΑΡΤΗΜΑ Β

Αναλυτικά αποτελέσματα βαθμού κινδύνων

Accommodation Moves	Κινήσεις στέγασης
Accounting	Λογιστική
Anti-spamming controls	Αντι-Spamming έλεγχοι
Application Input/Output Controls	Εισόδου-εξόδου έλεγχοι εφαρμογής
Audit	Λογιστικός έλεγχος
Back-up of Data	Υποστήριξη των στοιχείων
Business Continuity Planning	Προγραμματισμός επιχειρησιακής συνοχής
Capacity Planning	Προγραμματισμός ικανότητας
Compliance Checks	Έλεγχοι συμμόρφωσης
Content Scanning	Ικανοποιημένη ανίχνευση
Data Protection Legislation	Νομοθεσία προστασίας δεδομένων
Document / Media Controls	Έλεγχοι εγγράφων/μέσων
Equipment Failure Protection	Προστασία αποτυχίας εξοπλισμού
Fire Protection	Πυροπροστασία
Identification and Authentication	Προσδιορισμός και επικύρωση
Incident Handling	Συναφής χειρισμός
Insurance	Ασφάλεια
Logical Access Control	Λογικός έλεγχος προσπέλασης
Mobile Computing and Teleworking	Κινητοί υπολογισμός και τηλεργασία
Network Access Controls	Έλεγχοι προσπέλασης δικτύων
Network Security Management	Διαχείριση ασφάλειας δικτύων
Object Re-use	Επαναχρησιμοποίηση αντικειμένου
Personnel	Προσωπικό
Physical Equipment Protection	Προστασία Φυσικού εξοπλισμού
Power Protection	Προστασία Ρεύματος
Protection Against Malicious Software	Προστασία ενάντια στο κακόβουλο λογισμικό
Recovery Option for Hosts	Επιλογή αποκατάστασης για τους οικοδεσπότες
Recovery Options for Accommodation	Επιλογές αποκατάστασης για τη στέγαση
Security Education and Training	Εκπαίδευση και κατάρτιση ασφάλειας
Security Infrastructure	Υποδομή ασφάλειας
Security Policy	Πολιτική ασφαλείας
Security Testing	Δοκιμή ασφάλειας
Site / Building Physical Security	Περιοχή/φυσική ασφάλεια οικοδόμησης
Software Distribution	Διανομή λογισμικού
Software Integrity	Ακεραιότητα λογισμικού
System Administration Controls	Έλεγχοι διοίκησης συστημάτων
System Input/Output Controls	Εισόδου-εξόδου έλεγχοι συστημάτων
Theft Protection	Προστασία κλοπής