Βαλκανιώτης Τηλέμαχος (ΑΜ: mte1606)
Email: valkaniotist@gmail.com
Πανεπιστήμιο Πειραιώς
Ασφάλεια Ψηφιακών Συστημάτων

Διπλωματική εργασία
Συλλογή απαιτήσεων ασφαλείας και ιδιωτικότητας κατά την σχεδίαση συστημάτων

Υπεύθυνη δήλωση: Βεβαιώνω ότι είμαι συγγραφέας αυτής της πτυχιακής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της, είναι πλήρως αναγνωρισμένη και αναφέρεται στην πτυχιακή εργασία. Επίσης έχω αναφέρει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Επίσης βεβαιώνω ότι αυτή η διπλωματική εργασία προετοιμάστηκε από εμένα προσωπικά ειδικά για τις απαιτήσεις του προγράμματος μεταπτυχιακών σπουδών στην Ασφάλεια Ψηφιακών Συστημάτων του Τμήματος Ψηφιακών Συστημάτων του Πανεπιστημίου Πειραιώς.

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή μου, κύριο Κωνσταντίνο Λαμπρινουδάκη για την πτυχιακή αυτή και για την καθοδήγησή του κατά την εκπόνησή της. Θα ήθελα να ευχαριστήσω την οικογένειά μου η οποία με στήριξε ολοκληρωτικά στην απόφασή μου να συνεχίσω τις σπουδές μου μέχρι αυτό το επίπεδο καθώς επίσης να ευχαριστήσω τους φίλους μου στο Ηράκλειο οι οποίοι ήταν πάντα εκεί όταν τους χρειαζόμουν.

Περιεχόμενα

Πίνακας εικόνων

Πρόλογος

Ζούμε στο μέλλον. Τα συστήματα πληροφορικής μας προσφέρουν καθημερινά τις υπηρεσίες τους και διευκολύνουν την ζωή μας με τρόπους που δεν θα μπορούσαμε ποτέ να φανταστούμε. Πολύπλοκα συστήματα πληροφορικής φροντίζουν ώστε ασθενείς να παίρνουν την κατάλληλη φαρμακευτική αγωγή την κατάλληλη χρονική στιγμή. Συστήματα πληροφορικής υποστηρίζουν υπηρεσίες όπως ηλεκτρονική εξυπηρέτηση φορολογουμένων και άλλα ζητήματα τα οποία διευθετούνται με συστήματα ηλεκτρονικής διακυβέρνησης.

Η λειτουργία αυτών των συστημάτων απαιτεί δεδομένα. Ορισμένα συστήματα απαιτούν μεγάλους όγκους δεδομένων. Μερικά μπορεί να απαιτούν προσωπικά δεδομένα των χρηστών τους ή ακόμα και ευαίσθητα δεδομένα των χρηστών τους. Το δεύτερο στοιχείο που απαιτείται για να λειτουργεί όπως έχει σχεδιαστεί να λειτουργεί ένα σύστημα είναι η ασφάλειά του. Συνεπώς, αντιλαμβανόμαστε πως πρέπει να προστατέψουμε δύο ξεχωριστά πράγματα. Το σύστημα αυτό καθ' αυτό και τα δεδομένα τα οποία μπορεί να επεξεργάζεται.

Η πρώτη ερώτηση που εγείρεται στον αναγνώστη είναι γιατί πρέπει να προστατέψουμε το σύστημά μας αλλά και τα δεδομένα του. Οι λόγοι θα έπρεπε να είναι προφανής, αλλά θα αποπειραθούμε να εισάγουμε τον αναγνώστη στον κόσμο της ασφάλειας αναλύοντας επιγραμματικά τον λόγο που κάνει τον κόσμο να γυρίζει γύρω από τον εαυτό του. Ο κύριος και ίσως μοναδικός λόγος είναι ο οικονομικός παράγοντας. Ένα πληροφοριακό σύστημα επιταχύνει τις διαδικασίες ενός οργανισμού και τον βοηθά να επιτύχει τους στόχους του. Μπορεί να είναι μέρος των υπηρεσιών που προσφέρει ο οργανισμός ή να είναι η προσφερόμενη υπηρεσία. Κατ' επέκταση, τα δεδομένα που επεξεργάζεται το σύστημα, είναι μέρος αυτού. Αξίζει να σημειώσουμε πως το πληροφοριακό σύστημα με τα δεδομένα έχουν αλληλένδετη σχέση. Ένα πληροφοριακό σύστημα χωρίς δεδομένα είναι αδρανές και παραμένει αχρησιμοποίητο. Παρομοίως, δεδομένα χωρίς πληροφοριακό σύστημα το οποίο μπορεί να τα επεξεργαστεί δεν έχουν καμία απολύτως αξία.

Συμπεραίνουμε λοιπόν, πως η έκθεση ενός εκ των δύο σε κίνδυνο, θέτει σε άμεσο κίνδυνο τον ιδιοκτήτη οργανισμό. Προσβολή της ασφάλειας είτε των δεδομένων είτε του συστήματος, μπορεί να επιφέρει οικονομική ζημία με έμμεσο ή άμεσο τρόπο. Εάν ένα σύστημα δεν μπορεί λόγω κάποιου περιστατικού να προσφέρει τις υπηρεσίες του, μειώνεται η αξιοπιστία του οργανισμού και κατά συνέπεια θα μειωθούν και οι οντότητες που συναλλάσσονται με αυτόν. Ένα αμεσότερο οικονομικό χτύπημα στον οργανισμό μας μπορούν να επιφέρουν οι νομοθεσίες περί προστασίας των δεδομένων και των χρηστών ενός συστήματος που έχουν υιοθετηθεί από πολλά κράτη. Η παραβίαση της ιδιωτικότητας των χρηστών ενός συστήματος μπορεί να επιφέρει τεράστια οικονομικά πρόστιμα στον ιδιοκτήτη ενός συστήματος.

Αν τα δεδομένα των χρηστών ενός συστήματος είναι ασφαλή, μπορούμε επαγωγικά να ισχυριστούμε πως υπό αυτό το πρίσμα και οι χρήστες του συστήματός μας είναι ασφαλείς. Ο συγκεκριμένος όρος, παρότι είναι διαδεδομένος στο ευρύ κοινό χρηστών, καθώς και στην κοινότητα της πληροφορικής συνήθως μας φέρνει αντιμέτωπους με αντίμετρα τα οποία προστατεύουν τα δεδομένα κατά την διάρκεια της αποθήκευσής τους και μόνο. Σε αυτή την πτυχιακή θα εστιάσουμε περισσότερο στην ιδιωτικότητα των χρηστών, δηλαδή στο πόσο ασφαλείς είναι οι ίδιο οι χρήστες του συστήματος λόγω έκθεσης των δεδομένων τους κατά την μεταφορά τους από, προς και εντός του

συστήματός μας. Εφεξής θα χρησιμοποιείται ο όρος “privacy-aware σύστημα”, για να περιγραφθεί ένα σύστημα το οποίο φέρει κατάλληλα μέτρα προς επίτευξη της ιδιωτικότητας των χρηστών του.

Συνεπώς, όπως πιθανώς έχετε καταλάβει έως τώρα, η επένδυση σε μέτρα ασφαλείας και ιδιωτικότητας, δεν είναι επένδυση προσαύξησης κερδών ενός οργανισμού, αλλά ελαχιστοποίησης ζημίας σε περίπτωση εμφάνισης πιθανού περιστατικού. Αυτό βέβαια μπορεί να μην είναι πλήρως αληθές. Εάν οι χρήστες που χρησιμοποιούν το σύστημα γνωρίζουν πως το σύστημα και τα δεδομένα τους είναι ασφαλή καθώς επίσης πως το σύστημα αναγνωρίζει το δικαίωμα της ιδιωτικότητάς τους, θα έχουν θετική εντύπωση για αυτό. Καθ’ αυτό τον τρόπο μπορούν δυνητικά να λειτουργήσουν ως διαφήμιση του συστήματος αν αναλογιστούμε πως η θετική άποψη που θα αποκομίσουν επί του συστήματος, θα μεταδοθεί και σε χρήστες εκτός του συστήματος με συνέπεια την αύξηση των χρηστών. Υπό αυτή την σκοπιά, η επένδυση στην ασφάλεια και κατ’ επέκταση στον ασφαλή και privacy-aware σχεδιασμό συστημάτων, μπορεί να προσδιοριστεί και ως επένδυση η οποία μπορεί να αυξήσει τα κέρδη μίας εταιρίας.

Συνοψίζοντας τον πρόλογο, ελπίζουμε να έχουμε πείσει τον αναγνώστη να συνεχίσει την ανάγνωση αυτής της πτυχιακής, έχοντας του δημιουργήσει το εξής ερώτημα. Πως μπορούμε να σχεδιάσουμε και να κατασκευάσουμε ασφαλή συστήματα τα οποία εκτός από την σωστή και ασφαλή λειτουργία τους, θα λαμβάνουν υπόψιν την ιδιωτικότητα των χρηστών τους;

Σχόλιο [s1]: Τι γράφω ρε, χαραμίζομαι.. Κρατάω copyrights.

Κεφάλαιο 1

Εισαγωγή

1.0 Ορισμοί

Εν έτει 2017, με τον κλάδο της πληροφορικής να εξελίσσεται σε ραγδαίους ρυθμούς, να προσφέρει γνώση και υπηρεσίες σε ένα ολοένα και αυξανόμενο πλήθος κόσμου, τα συστήματα πληροφορικής δεν έχουν άλλη επιλογή από το να ακολουθήσουν αυτές τις κλίσεις και συνεπώς να αυξηθούν και αυτά ώστε να ικανοποιήσουν την ζήτηση.

Μέρος όλης της προσφερόμενης γνώσης που προσφέρεται από πληροφοριακά συστήματα όπως το Internet, αποτελούν και τρόποι με τους οποίους μπορεί κανείς να εκθέσει ένα πληροφοριακό σύστημα και πολλές φορές εν συνεχεία να προσβάλλει την ιδιωτικότητα των χρηστών του συστήματος διαρρέοντας προσωπικά τους δεδομένα τα οποία πιθανώς να διαχειριζόταν το σύστημα, προς τρίτους. Μπορούμε συνεπώς να αποδεχθούμε το γεγονός πως λόγω μη έλλειψης γνώσεων και κινήτρων όπως η απλή περιέργεια ή το οικονομικό όφελος, οι κυβερνοεπιθέσεις απέναντι στα πληροφοριακά συστήματα δεν πρόκειται να μειωθούν.

Σύμφωνα με το RFC 2828 (1), μία επίθεση σε ένα υπολογιστικό σύστημα την οποία πραγματοποιεί μία νοήμων οντότητα, είναι η εσκεμμένη ενέργεια που αποσκοπεί στο να παραβιάσει την πολιτική ασφαλείας ενός συστήματος. Μία τέτοια ενέργεια μπορεί να εκθέσει την ακεραιότητα, την εμπιστευτικότητα αλλά και την διαθεσιμότητα του συστήματος. Η επίθεση που χρησιμοποιεί ως μέσο πραγματοποίησής της όχι μόνο κάποιον ηλεκτρονικό υπολογιστή, αλλά και το Internet, ονομάζεται κυβερνοεπίθεση. Οι επιθέσεις που θα μας απασχολήσουν σε αυτή την διπλωματική εργασία θα αφορούν όχι μόνο την ασφάλεια του συστήματος, αλλά και την ιδιωτικότητα των χρηστών αυτού.

Στο έγγραφο του NIST περί πληροφορίας και πληροφοριακών συστημάτων (2) η τριάδα εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας αφορούν και τα δεδομένα και τα πληροφοριακά συστήματα και οι όροι εμπιστευτικότητα και ιδιωτικότητα χρησιμοποιούνται ενναλακτικά. Σε αυτή την πτυχιακή ο όρος ιδιωτικότητα θα εξεταστεί ξεχωριστά, επομένως η τριάδα ακεραιότητας, εμπιστευτικότητας και διαθεσιμότητας θα αφορά αποκλειστικά τα πληροφοριακά συστήματα.

Σχόλιο [s2]: Αφρούς ο Καλλονιάτης.

Πάλι σύμφωνα με το (2) η εμπιστευτικότητα ορίζεται ως η διατήρηση των καθορισμένων περιορισμών ως προς την πρόσβαση και αποκάλυψη των δεδομένων ενός συστήματος, συμπεριλαμβανομένων των μέτρων που λαμβάνονται για την προστασία την ιδιωτικότητας των χρηστών αλλά και ιδιόκτητων δεδομένων. Ακεραιότητα θα ονομάσουμε την ιδιότητα ενός συστήματος να διαφυλάσσεται ενάντια σε αθέμιτες τροποποιήσεις και την αθέμιτη καταστροφή δεδομένων καθώς επίσης και η διαφύλαξη της ιδιότητας της αυθεντικότητας αλλά και της μη αποποίησης των δεδομένων σε σχέση με τον ιδιοκτήτη τους. Τέλος, διαθεσιμότητα θα ορίσουμε την εξασφάλιση πως η πρόσβαση και η χρήση ενός συστήματος από τους χρήστες του θα πραγματοποιείται ανεμπόδιστα. Αυτοί οι 3 όροι χρησιμοποιούνται για να αναφερθούμε στην ασφάλεια ενός συστήματος αλλά και των πληροφοριών.

Οι όροι που χρησιμοποιούνται για να καθορίσουμε τις ανάγκες μας ως προς την ιδιωτικότητα των χρηστών ενός συστήματος είναι οι εξής (3):

- Ανωνυμία
- Ψευδωνυμία
- Μη-συνδεσιμότητα
- Μη-ανιχνευσιμότητα
- Μη-παρατηρησιμότητα

Ο ορισμός της ανωνυμίας καθορίζει πως αν ένα αντικείμενο επιθυμεί να φέρει την ιδιότητα της ανωνυμίας θα πρέπει να είναι μη αναγνωρίσιμο ανάμεσα στα υπόλοιπα αντικείμενα τα οποία επιθυμούν να φέρουν αυτή την ιδιότητα επίσης. Για παράδειγμα αν ο παραλήπτης ενός μηνύματος επιθυμεί να ξέρει ποιος είναι ο αποστολέας του, θα είναι σε θέση να αναγνωρίσει το ανώνυμο σύνολο στο οποίο ανήκει ο παραλήπτης αλλά δεν θα βρίσκεται σε θέση να τον ξεχωρίσει από το σύνολο. (4)

Ως ψευδωνυμία ορίζεται η χρήση ψεύτικων ονομάτων από οντότητες που θέλουν να επικοινωνήσουν. Τα ψευδώνυμα μπορούν να χρησιμοποιούνται ώστε να υπάρχει η ικανότητα επικοινωνίας μεταξύ 2 οντοτήτων όταν δεν θέλουν να αποκαλύπτεται η πραγματική τους ταυτότητα. (4)

Η ιδιότητα της μη-συνδεσιμότητας, αναφέρεται στην ιδιότητα ενός συστήματος να αποκρύπτει συνδέσεις μεταξύ αντικειμένων ενδιαφέροντος από κάποιο επιτιθέμενο μέσα σε ένα καθορισμένο πλαίσιο εντός του συστήματος υπό επίθεση. Τα αντικείμενα ενδιαφέροντος μπορεί να αναφέρονται σε φυσικές οντότητες του συστήματος (χρήστες), σε μηνύματα τα οποία μεταφέρονται εντός του συστήματος ή σε ενέργειες των χρηστών του συστήματος. (4)

Ο όρος της μη ανιχνευσιμότητας χρησιμοποιείται για να περιγράψει την ιδιότητα ενός συστήματος να εισάγει αμφιβολία στον επιτιθέμενο ως προς την ύπαρξη αντικειμένων ενδιαφέροντος μέσα σε ένα σύστημα. Ο επιτιθέμενος μπορεί να βρίσκεται εντός ή εκτός του συστήματος και να έχει a-priori γνώση επί αυτού, δηλαδή να γνωρίζει για την ύπαρξη πιθανών αντικειμένων ενδιαφέροντος, αλλά να μην μπορεί να αποδείξει την ύπαρξή τους εντός του συστήματος. (4)

Στο (5) η μη-παρατηρησιμότητα ορίζεται η ικανότητα ενός χρήστη του συστήματος να χρησιμοποιήσει μία υπηρεσία χωρίς να μπορεί κάποιος να αποδείξει πως γίνεται χρήση αυτής της υπηρεσίας από τον οποιοδήποτε την συγκεκριμένη χρονική στιγμή. Το (4) θέτει την μη παρατηρησιμότητα ως τον συνδυασμό μη-ανιχνευσιμότητας και ανωνυμίας ενός αντικειμένου ενδιαφέροντος. Συνεπώς αν ένα αντικείμενο βρίσκεται υπό την ομπρέλα μέτρων τα οποία εξασφαλίζουν την μη-ανιχνευσιμότητα του αλλά και την ανωνυμία του, μπορούμε να ισχυριστούμε πως είναι εξασφαλισμένη και η μη παρατηρησιμότητα του.

Ο ασφαλής και privacy-aware σχεδιασμός ενός συστήματος έχει ως κέντρο βάρους τους όρους που αναλύσαμε παραπάνω. Βάσει απαιτήσεων του συστήματος, ο σχεδιαστής του συστήματος θα κληθεί να διαλέξει τα κατάλληλα μέτρα ώστε να ικανοποιηθούν οι ανάγκες για ασφάλεια και ιδιωτικότητα. Αυτό όμως δεν σημαίνει πως θα πρέπει να επιλεχθούν και εφαρμοστούν μέτρα για όλους τους όρους που προαναφέραμε. Τα μέτρα καθορίζονται βάσει αναγκών του συστήματος οι οποίες εμφανίζονται κατά την νοητή σύλληψη του όλου συστήματος. Συνεπώς, αν ο ιδιοκτήτης του συστήματος απαιτεί μόνο την ακεραιότητα του συστήματος και τίποτα άλλο, ο σχεδιαστής θα πρέπει να λάβει μέτρα για να εξασφαλίσει την ακεραιότητα και μόνο.

1.1 Περίληψη

Στο πρώτο κεφάλαιο εξετάσαμε τους όρους ιδιωτικότητα και ασφάλεια και αναλύσαμε ποιες είναι οι απαιτήσεις που μπορεί να κληθεί να ικανοποιήσει ένας σχεδιαστής. Επίσης για κάθε μία απαίτηση δώσαμε έναν σύντομο ορισμό, προς διευκόλυνση του αναγνώστη.

Στο κεφάλαιο δύο, θα αναφερθούμε στον ορισμό του συστήματος, θα δούμε τα στοιχεία που το αποτελούν αλλά και πως συνδέονται μεταξύ τους, καθώς επίσης και πως συνδέονται με τα συστήματα πληροφορικής. Στο δεύτερο μέρος του κεφαλαίου, θα εξετάσουμε την μηχανική απαιτήσεων και πως αυτή βοηθάει στον σχεδιασμό ενός πληροφοριακού συστήματος.

Το τρίτο κεφάλαιο είναι αφιερωμένο στην διαχείριση κινδύνου. Θα εξηγήσουμε τις βασικές έννοιες, θα εξετάσουμε τα διάφορα είδη κινδύνου, θα γίνει ανάλυση της διαδικασίας διαχείρισης κινδύνου, καθώς και επί μέρους ανάλυση του κάθε βήματος ξεχωριστά. Τέλος, θα εξετάσουμε την μεθοδολογία διαχείρισης κινδύνου EBIOS.

Στην συνέχεια θα μελετήσουμε την ασφαλειοστραφή μεθοδολογία ανάπτυξης λογισμικού SecureTropos, θα παραθέσουμε τους ορισμούς της και θα δώσουμε επεξηγήσεις για τα διάφορα σύμβολα που χρησιμοποιεί. Επίσης θα δώσουμε παραδείγματα εφαρμογής της μεθοδολογίας, μέσω του εργαλείου SecTro το οποίο έχει αναπτυχθεί από τους εμπνευστές της SecureTropos.

Το κεφάλαιο νούμερο πέντε μιλάει για την μεθοδολογία Pris και το πως προσπαθεί να λύσει το πρόβλημα της έλλειψης της νοοτροπίας ιδιωτικότητας στην πρώιμη σχεδίαση ενός πληροφοριακού συστήματος. Όπως και με την SecureTropos, θα εξηγήσουμε τους ορισμούς που την διέπουν και θα περιγράψουμε τα όποια στάδια την απαρτίζουν.

Στο έκτο κεφάλαιο θα κάνουμε χρήση όλων των μεθοδολογιών που εξετάσαμε στα προηγούμενα κεφάλαια και θα τα εφαρμόσουμε πάνω σε ένα σύστημα ανταλλαγής πληροφοριών οχημάτων, παρουσιάζοντας ταυτοχρόνως την μεθοδολογία SaferTec η οποία χρησιμοποιεί της προηγούμενες μεθοδολογίες υπό ένα κοινό πλαίσιο.

Τέλος στο κεφάλαιο εφτά, θα παραθέσουμε τα συμπεράσματά μας για τις μεθοδολογίες που εξετάσθηκαν και θα αναφερθούμε σε μελλοντικά πεδία έρευνας που θα ήταν ενδιαφέρουσα η έρευνά τους.

Κεφάλαιο 2

Θεωρία Συστημάτων

2.1 Ορισμός

Δεν γίνεται να αποπειραθούμε να προστατέψουμε την ασφάλεια και την ιδιωτικότητα ενός συστήματος, εάν δεν γνωρίζουμε έως ένα βάθος τι είναι ένα σύστημα πληροφορικής. Ένα σύστημα πληροφορικής, υπόκειται στην γενικότερη κατηγορία συστημάτων και ως φυσικό επόμενο χαρακτηρίζεται από τις βασικές έννοιες που καθορίζουν ένα σύστημα. Για να μελετήσουμε και να κατανοήσουμε ένα σύστημα πληροφορικής, πρέπει πρώτα να καταλάβουμε τι είναι ένα σύστημα, ποια είναι τα στοιχεία που το αποτελούν και πότε καθορίζουμε μία οντότητα ως σύστημα. Στην συνέχεια θα αποπειραθούμε να εξηγήσουμε πως γίνεται η θεωρητική μεταβίβαση από ένα γενικό σύστημα σε ένα σύστημα πληροφορικής.

Ο όρος σύστημα προέρχεται από την αρχαία ελληνική λέξη συνίστημι, η οποία σημαίνει “να αποκτώ μορφή, να συγκρατώ”. Το 1968 ο Ludwig von Bertalanffy εκδίδει το έργο του “General Systems Theory” (6) στο οποίο αναγράφεται η πρώτη ολοκληρωμένη θεωρία συστημάτων. Σε αυτό το έργο, ο Ludwig von Bertalanffy καταφέρνει να τοποθετήσει όλα τα συστήματα, για τα οποία υπήρχαν ήδη θεωρίες, υπό ένα κοινό πλαίσιο. Μέχρι τότε υπήρχαν θεωρίες ξεχωριστές θεωρίες για διάφορα συστήματα, όπως τα μηχανικά ή τα κοινωνικά συστήματα, τα οποία με την συγκεκριμένη θεωρία κατάφεραν να συνδεθούν μεταξύ τους.

Σκοπός του “General Systems Theory” και κατ’ επέκταση του Ludwig von Bertalanffy ήταν να προτείνει έναν νέο τρόπο να γίνεται η επιστημονική έρευνα. Στο κεφάλαιο “Aims of General Systems Theory” αναφέρει πως είχε παρατηρήσει πως υπήρχαν παρόμοια μοτίβα και οπτικές γωνίες για πεδία της επιστήμης τα οποία δεν έχουν σχέση μεταξύ τους. Κάνει λόγο για γεγονότα ή προβλήματα στην έρευνα των ήδη υπαρχόντων συστημάτων. Πιο συγκεκριμένα αναφέρει πως η μελέτη ξεχωριστών μερών των συστημάτων υπό έρευνα, προβλημάτιζε την επιστημονική κοινότητα ως προς την κατανόησή τους.

Η παρατήρηση των κοινών ιδεών σε επιστημονικά πεδία ανεξάρτητα το ένα από το άλλο, ήταν αυτή που γέννησε την θεωρία συστημάτων. Η θεωρία συστημάτων είναι η επιστήμη της ολότητας. Μέσω αυτής μπορούμε να αναγνωρίσουμε κοινά σημεία σε διαφορετικά επιστημονικά πεδία. Έτσι γίνεται ευκολότερη η κατανόηση του πεδίου, δεδομένης προ υπάρχουσας γνώσης σε κάποιο άλλο πεδίο. Αυτός ήταν ένας από τους στόχους τους οποίους ήθελε να επιτύχει ο Ludwig von Bertalanffy. Ο κυριότερος στόχος της θεωρίας του, ήταν η σύγκλιση των επιστημονικών πεδίων.

Το μοντέλο ενός συστήματος είναι απλό και τα μέρη τα οποία το απαρτίζουν είναι αρκετά αφηρημένης έννοιας ώστε να ταιριάζουν σε όλα τα συστήματα. Κυρίαρχες έννοιες του μοντέλου είναι οι εξής:

- Διεγερτικός παράγοντας
- Αισθητήριο όργανο
- Μηχανισμός ελέγχου
- Επενεργητής
- Μήνυμα
- Απόκριση

- Ανατροφοδότηση

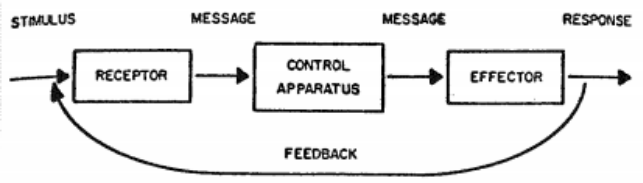
Ο διεγερτικός παράγοντας είναι η οντότητα που ενεργοποιεί ένα σύστημα και το προκαλεί να εκτελέσει τις διαδικασίες το οποίο είναι σχεδιασμένο να εκτελεί. Χωρίς αυτόν, το σύστημα υφίσταται, αλλά βρίσκεται σε αδράνεια.

Μπορούμε να έχουμε διεγερτικό παράγοντα, αλλά χρειαζόμαστε ένα αισθητήριο όργανο ώστε να αντιληφθούμε την ύπαρξη του διεγερτικού παράγοντα. Η δεύτερη ευθύνη του αισθητηρίου οργάνου είναι να ενημερώσει την διαδικασία ελέγχου για τον διεγερτικό παράγοντα που τυχόν ανίχνευσε.

Ο μηχανισμός ελέγχου είναι το νευραλγικό κέντρο όλου του μοντέλου. Βάσει του μηνύματος που θα λάβει από το αισθητήριο όργανο, θα πρέπει να αποφασίσει για την φύση του μηνύματος που θα αποστείλει στον κατάλληλο επενεργητή.

Ο επενεργητής είναι η προσωποποίηση, η υλική υπόσταση της απόφασης του μηχανισμού ελέγχου. Είναι η οντότητα που θα προσφέρει το αποτέλεσμα, την απόκριση αν θέλετε, των προηγούμενων μερών σε άλλα περιβάλλοντα ή συστήματα, αλλά και στο ίδιο περιβάλλον μέσω της ανατροφοδότησης.

Ανατροφοδότηση ονομάζουμε την διαδικασία κατά την οποία η απόκριση που έχει παραχθεί από τον μηχανισμό ελέγχου και μεταδοθεί από τον επενεργητή, επιστρέφει στο αισθητήριο όργανο με αποτέλεσμα να επηρεάζει τον επόμενο διαδικαστικό κύκλο.



ΕΙΚΟΝΑ 1 ΜΟΝΤΕΛΟ ΣΥΣΤΗΜΑΤΟΣ

2.2 Συστήματα πληροφορικής

Δεδομένου πως τα συστήματα πληροφορικής είναι υποσύνολα των συστημάτων, είναι αναμενόμενο να δανείζονται στοιχεία από αυτό. Είναι επίσης φυσικό να εισάγονται νέα στοιχεία που δεν υπήρχαν στο πρωταρχικό μοντέλο. Συνεπώς είμαστε αναγκασμένοι να αναγνωρίσουμε ποια είναι αυτά τα νέα στοιχεία που δομούν το πληροφοριακό σύστημα καθώς επίσης και να αντιστοιχήσουμε τα στοιχεία που κληρονομούνται από το πρωταρχικό μοντέλο.

Ο διεγερτικός παράγοντας μετατρέπεται στους χρήστες του συστήματος. Οι χρήστες είναι αυτοί οι οποίοι θα αλληλοεπιδρούν με το σύστημά μας δίνοντάς του ζωή και λόγο ύπαρξης. Δεν είναι όμως και οι μόνοι. Αναλόγως την φύση του συστήματος, μπορεί να υπάρχει επικοινωνία και με άλλα συστήματα προς προσφορά υπηρεσιών ή ακόμα και υποδομών. Για αυτό τον λόγο, θα ορίσουμε ως διεγερτικό παράγοντα του πληροφοριακού συστήματος οποιαδήποτε οντότητα επικοινωνήσει με αυτό, απαιτώντας υπηρεσίες ή υποδομές.

Ως αισθητήρια όργανα μπορούμε να θεωρήσουμε τα σημεία του συστήματος τα οποία δέχονται δεδομένα προς επεξεργασία. Μία φόρμα σε μία ιστοσελίδα, ή ένα endpoint (τελικό σημείο) προγραμματιστικής διεπαφής μπορούν να θεωρηθούν αισθητήρια όργανα του συστήματος. Στην ορολογία των συστημάτων πληροφορικής, αυτό το στοιχείο μετονομάζεται σε σημείο εισόδου.

Ο μηχανισμός ελέγχου υφίσταται και στο πληροφοριακό σύστημα. Είναι το τμήμα του λογισμικού το οποίο ευθύνεται να πραγματοποιήσει την επεξεργασία των δεδομένων που έλαβε από τα σημεία εισόδου. Όλο το backend κομμάτι ενός συστήματος, μπορεί να θεωρηθεί μηχανισμός ελέγχου του συστήματος. Εφόσον γίνει η απαραίτητη επεξεργασία, αναλόγως με τον προγραμματισμό του, ο μηχανισμός ελέγχου είναι υπεύθυνος είτε να αποστείλει τα απαραίτητα δεδομένα προς την πρέπουσα οντότητα. Συνήθως οι οντότητες με τις οποίες συναλλάσσεται ένας μηχανισμός ελέγχου είναι το σύστημα αποθήκευσης δεδομένων στο οποίο θα αναφερθούμε στην συνέχεια και τα σημεία εξόδου του συστήματος.

Το πληροφοριακό σύστημα, μετά το πέρας της επεξεργασίας του αιτήματος που τυχόν έλαβε, οφείλει να ενημερώσει τον χρήστη για το αποτέλεσμα του αιτήματός του. Αυτό μπορεί να συμβεί είτε προσφέροντάς του κάποια ένδειξη επιτυχούς η μη ολοκλήρωσης του αιτήματος. Στην πλειοψηφία των περιπτώσεων, μία επιτυχημένη επεξεργασία δεδομένων από τον μηχανισμό ελέγχου, το πληροφοριακό σύστημα αποστέλλει παραπάνω πληροφορία από την δυική φύση της ένδειξης ολοκλήρωσης ή μη ολοκλήρωσης ενός αιτήματος. Αυτή η πληροφορία είναι το παράγωγο του μηχανισμού ελέγχου και ορισμένες περιπτώσεις, μπορεί να καθορίζει την εξέλιξη των επόμενων κινήσεων του αιτούντος συστήματος.

Σχόλιο [s3]: ΧΑΡΑΜΙΖΟΜΑΙ στο Ελλαδιστάν.

Το νέο κομμάτι το οποίο κάνει την είσοδό του στην σκηνή των μοντέλων συστημάτων είναι οι μηχανισμοί αποθήκευσης δεδομένων. Τα δεδομένα που εισέρχονται διαμέσου των endpoints του συστήματος, ενδέχεται μετά την επιτυχημένη επεξεργασία τους να απαιτείται η αποθήκευσή τους από το σύστημα προς εξυπηρέτηση μελλοντικών αιτημάτων. Κάλλιστα θα μπορεί ο σκοπός ενός συστήματος να είναι η προσφορά αποθηκευμένης πληροφορίας στους αιτούντες. Για αυτό τον σκοπό, απαιτείται η ύπαρξη κάποιου μηχανισμού ο οποίος θα είναι υπεύθυνος για την διαφύλαξη αυτών των δεδομένων.

2.3 Μηχανική απαιτήσεων

Οι απαιτήσεις ενός συστήματος είναι η περιγραφή του τι πρέπει να κάνει ένα σύστημα. Τις υπηρεσίες που πρέπει να προσφέρει, αλλά και τους περιορισμούς που θα έχει κατά την λειτουργία του. Αυτές οι απαιτήσεις αντικατοπτρίζουν τις προσδοκίες ενός χρήστη του συστήματος και πως το σύστημα ανταπεξέρχεται σε αυτές. Η διαδικασία της εύρεσης, ανάλυσης, καταγραφής και ελέγχου πλήρωσης απαιτήσεων και περιορισμών, ονομάζεται μηχανική απαιτήσεων. (7)

Μερικά από τα προβλήματα που αναδύονται κατά διαδικασία της μηχανικής απαιτήσεων είναι αποτέλεσμα της αποτυχίας μας να διαχωρίσουμε τις διαφορετικές απαιτήσεις του συστήματος καταλλήλως. Προς βοήθειά μας, χωρίζουμε τις απαιτήσεις σε απαιτήσεις του συστήματος και απαιτήσεις των χρηστών

Οι απαιτήσεις των χρηστών περιγράφονται ως δηλώσεις στην φυσική γλώσσα και περιγράφουν τις υπηρεσίες που οφείλει να προσφέρει ένα σύστημα στους χρήστες του, αλλά και τους περιορισμούς υπό τους οποίους θα προφέρει τις εν λόγω υπηρεσίες.

Οι απαιτήσεις του συστήματος είναι λεπτομερείς περιγραφές του λογισμικού που υλοποιεί το σύστημα, τις υπηρεσίες που προσφέρονται και τους επιχειρησιακούς περιορισμούς. Οι απαιτήσεις του συστήματος οφείλουν να περιγράφουν με κάθε λεπτομέρεια το τι πρόκειται να εφαρμοστεί προς ολοκλήρωση του συστήματος.

Ας πάρουμε για παράδειγμα ένα σύστημα διαχείρισης φαρμάκων σε μία κλινική. Ας υποθέσουμε πως μία κλινική, ζητάει να παράγονται μηνιαίες αναφορές διαχείρισης κόστους των φαρμάκων που προσφέρει. Αυτή η γενική δήλωση, αποτελεί απαίτηση χρήστη. Μας ζητούν επίσης

συγκεκριμένες υπηρεσίες που πρέπει να προσφέρει το σύστημα τις οποίες και καταγράφουν στην κήρυξη του έργου τους. Μπορεί να θέλουν συγκεκριμένη ώρα και ημέρα να παράγεται αναφορά, ή το σύστημα να τους ειδοποιεί για τα αποθέματα φαρμάκων που υπάρχουν στην αποθήκη. Αυτές οι δηλώσεις μπορούν να χαρακτηρισθούν ως απαιτήσεις συστήματος.

Οι απαιτήσεις του συστήματος, μπορούν να διαχωρισθούν περαιτέρω στα 2 εξής πεδία. Τις λειτουργικές και τις μη λειτουργικές απαιτήσεις. Οι λειτουργικές απαιτήσεις καθορίζουν τις υπηρεσίες του συστήματος, την συμπεριφορά του σε συγκεκριμένες καταστάσεις αλλά και την απόκριση που πρέπει να δίνει σε συγκεκριμένα ερεθίσματα (inputs). Οι μη λειτουργικές απαιτήσεις είναι οι περιορισμοί που διέπουν ένα σύστημα. Παραδείγματα περιορισμών σε ένα σύστημα μπορεί να είναι οι προσφερόμενες υπηρεσίες ανάλογα τον τύπο του χρήστη ή περιορισμοί που θέτονται από standards. Συνήθως οι μη λειτουργικές απαιτήσεις διέπουν ολόκληρο το σύστημα και όχι μεμονωμένες υπηρεσίες του.

2.4 Διαδικασίες μηχανικής απαιτήσεων

Η μηχανική απαιτήσεων περιλαμβάνει 4 διαδικασίες οι οποίες πραγματοποιούνται κατά την διάρκεια της ανάπτυξης ενός συστήματος οι οποίες είναι οι εξής:

- Μελέτη σκοπιμότητας
- Ανάλυση απαιτήσεων
- Προσδιορισμός απαιτήσεων
- Επικύρωση απαιτήσεων

Κατά την διάρκεια της μελέτης σκοπιμότητας γίνεται ανάλυση του ήδη υπάρχοντος συστήματος. Με το πέρας της μελέτης θα πρέπει να υπάρχει ένα ξεκάθαρο συμπέρασμα για το αν το σύστημα θα είναι οικονομικώς βιώσιμο από πλευράς της εταιρίας και αν μπορεί να κατασκευαστεί με τον υπάρχοντα προϋπολογισμό. Βάσει αυτού του συμπεράσματος, αποφασίζουμε αν μπορούμε να προχωρήσουμε στην επόμενη φάση, στην ανάλυση των απαιτήσεων του συστήματος.

2.4.1 Ανάλυση απαιτήσεων

Η διαδικασία της ανάλυσης απαιτήσεων είναι η διαδικασία κατά την οποία εξάγουμε και κατανοούμε τις απαιτήσεις του συστήματος. Αυτό γίνεται μέσω επικοινωνίας με τους πιθανούς χρήστες του, με τα ενδιαφερόμενα μέρη του, αλλά και τους πιθανούς προμηθευτές του συστήματος. Δεν είναι επίσης σπάνιο φαινόμενο να κατασκευάζεται κάποιου είδους πρωτότυπο σύστημα για λόγους επίδειξης, γεγονός το οποίο επιταχύνει την διαδικασία της ανάλυσης, καθώς δύναται να υπάρξει ανατροφοδότηση από πρόωρους δοκιμαστές του συστήματος, κάτι το οποίο οδηγεί σε γρηγορότερη κατανόηση των απαιτήσεων.

Σχόλιο [s4]: Ας με σταματήσει κάποιος.

Η συγκεκριμένη διαδικασία έχει από μόνη της αρκετές διαδικασίες οι οποίες πρέπει να πραγματοποιηθούν. Αρχικά πρέπει να ανακαλύψουμε ποιες είναι οι απαιτήσεις του συστήματος, λειτουργικές και μη λειτουργικές. Θεωρείται μία εκ των δυσκολότερων φάσεων κατά της διάρκεια της ανάλυσης απαιτήσεων. Αυτό συμβαίνει καθώς υπάρχει πλήθος οντοτήτων το οποίο εμπλέκεται στην διαδικασία παραδείγματα των οποίων είναι, ενδοεταιρικοί παράγοντες, συνήθως οικονομικής ή ιεραρχικής φύσεως, διαφορετικές ή/και αντικρουόμενες απαιτήσεις από διαφορετικά ενδιαφερόμενα μέρη αλλά ακόμα και η ίδια η άγνοια των ενδιαφερόντων μερών, επί την φύση των απαιτήσεων. Η ανακάλυψη απαιτήσεων συνήθως γίνεται μέσω συνεντεύξεων με τα ενδιαφερόμενα μέρη. Επίσης χρησιμοποιούνται μοντέλα και σχηματικές αναπαραστάσεις που αναπαριστούν το σύστημα κατά την ολοκλήρωσή του, καθώς γίνεται χρήση σεναρίων προς πλήρη κατανόηση της πλήρους λειτουργίας του συστήματος.

Εν συνεχεία πραγματοποιείται κατηγοριοποίηση των απαιτήσεων. Ορισμένες απαιτήσεις μπορεί να υλοποιούνται σε παραπλήσια ή αν όχι στα ίδια υποσυστήματα. Στηριζόμενοι στις κατηγορίες των απαιτήσεων μπορούμε να λάβουμε καλύτερες αποφάσεις για την ανάθεση πόρων προς ολοκλήρωσή τους. Οι ομάδες που θα αναλάβουν την υλοποίηση των απαιτήσεων δεν θα χρειάζεται να διαφοροποιούν το νοητικό τους πλαίσιο εντελώς κάθε φορά που θα ολοκληρώνουν μία απαίτηση και αυτό μπορεί να οδηγήσει σε αύξηση της παραγωγικότητάς τους.

Σχόλιο [s5]: Δώστε μου ένα Pullinger, έστω ένα leadership & management award.

Μία άλλη διαδικασία για την ανάλυση απαιτήσεων αποτελεί η απόδοση προτεραιότητας σε κάθε κατηγορία απαιτήσεων. Όταν εμπλέκονται πολλαπλά μέρη σε ένα σύστημα, μπορεί να υπάρξουν διενέξεις μεταξύ τους. Δίνοντας προτεραιότητα σε κάποια απαίτηση, αυτή αποκτά βάρος. Έτσι, αν υπάρχει κάποια διένεξη κατά την εφαρμογή της απαίτησης, μπορούμε να αποφασίσουμε γρηγορότερα και ευκολότερα ως προς το ποια θα είναι η συνέχεια των ενεργειών μας.

2.4.2 Προσδιορισμός απαιτήσεων

Αυτό που έπεται της διαδικασίας ανάλυσης, είναι η διαδικασία προσδιορισμού απαιτήσεων. Κατά την διάρκεια αυτής της διαδικασίας χρησιμοποιούμε την συλλεχθείσα πληροφορία της προηγούμενης φάσης και συντάσσουμε ένα έγγραφο το οποίο προσδιορίζει τις απαιτήσεις του συστήματος. Υπό ιδανικές συνθήκες, οι απαιτήσεις ενός συστήματος θα πρέπει να καταγράφονται με τρόπο ξεκάθαρο και ευνόητο προς τα ενδιαφερόμενα μέρη. Στην πράξη, αυτή η διαδικασία συνήθως βγάζει στην επιφάνεια αρκετές διενέξεις μεταξύ των ενδιαφερόμενων μερών όσων αφορά την λειτουργικότητα του συστήματος και πως αυτή επιτυγχάνεται.

Συγχρόνως οι καταγεγραμμένες απαιτήσεις δεν θα πρέπει να είναι αρκετά τεχνικές. Θα πρέπει να παρουσιάζουν στον αναγνώστη μία αφαιρετική εικόνα της λειτουργίας του συστήματος χωρίς να εμβαθύνει σε τεχνικές λεπτομέρειες. Αυτή η προσέγγιση φαντάζει ιδανική, όμως εγείρονται προβλήματα που μας αποτρέπουν από το να καταγράψουμε εντελώς αφαιρετικά τις απαιτήσεις του συστήματος. Αυτά τα προβλήματα μπορεί να είναι η επικοινωνία μεταξύ υποσυστημάτων αλλά ακόμα και η ίδια η αρχιτεκτονική του συστήματος.

Η φυσική γλώσσα και τα διαγράμματα UML (Unified Modeling Language) είναι τα 2 κύρια μέσα που χρησιμοποιούμε για να προσδιορίσουμε και να καταγράψουμε τις απαιτήσεις του συστήματος. Η φυσική γλώσσα μας εξυπηρετεί εξαιρετικά στην περιγραφή και τον ορισμό των απαιτήσεων, ενώ τα διαγράμματα UML είναι χρήσιμα στο να περιγράφουν τις διάφορες φάσεις στις οποίες μπορεί να περιέλθει το σύστημά μας και πως γίνεται η μετάβαση από την μία φάση στην άλλη.

2.4.3 Επικύρωση απαιτήσεων

Τέλος, κατά την διάρκεια επικύρωσης των απαιτήσεων γίνεται επανεξέταση των απαιτήσεων του συστήματος όπως ο ρεαλισμός τους, η συνέχειά τους ή η ολότητά τους. Αν κάποια από τις απαιτούμενες ιδιότητες δεν πληρείται από κάποια απαίτηση, γίνεται επανεκκίνηση ολόκληρης της διαδικασίας, για την συγκεκριμένη απαίτηση και μόνο. Αν μία απαίτηση επηρεάζει άλλες απαιτήσεις, οφείλουμε να επαναλάβουμε την διαδικασία και για αυτές.

Η επικύρωση απαιτήσεων θα μπορούσε να απορροφηθεί από την διαδικασία ανάλυσης απαιτήσεων καθώς οι διαδικασίες μοιάζουν αρκετά. Οφείλουμε να αναφερθούμε ξεχωριστά σε αυτή και να της αφιερώσουμε ξεχωριστό κομμάτι καθώς κατά την επικύρωση απαιτήσεων, πραγματοποιούνται οι εξής διαδικασίες:

- Έλεγχος επικύρωσης
- Έλεγχος συνέχειας
- Έλεγχος ολότητας

- Έλεγχος ρεαλισμού
- Επαλήθευση

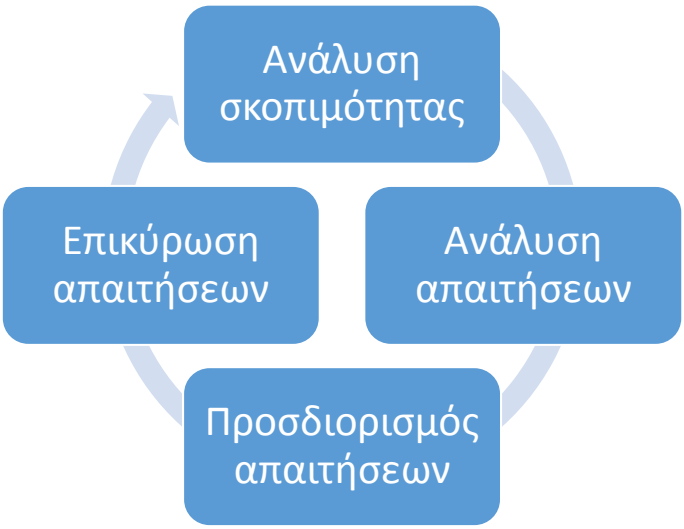
Κατά τον έλεγχο επικύρωσης, τα μέρη που έχουν αναλάβει την κατασκευή του συστήματος επιβεβαιώνουν μαζί με τα ενδιαφερόμενα μέρη του συστήματος τις απαιτήσεις. Συνήθως δεν υπάρχουν διαφοροποιήσεις απαιτήσεων. Η πιθανότητα όμως δεν είναι μηδενική, συνεπώς οφείλουμε να πραγματοποιούμε αυτό τον έλεγχο.

Ο έλεγχος συνέχειας είναι η διαδικασία κατά την οποία εξετάζουμε τις απαιτήσεις για να ανακαλύψουμε τυχόν διενέξεις που μπορεί να υπάρχουν ανάμεσα στις λειτουργικές απαιτήσεις του συστήματος μεταξύ τους, είτε ανάμεσα στις λειτουργικές και τις μη λειτουργικές απαιτήσεις. Τυχόν διενέξεις πρέπει να λύνονται προτού συνεχιστεί η κατασκευή του συστήματος.

Ο έλεγχος ολότητας αναλαμβάνει να ελέγξει αν έχουν ληφθεί υπόψιν όλες οι λειτουργικές και μη λειτουργικές απαιτήσεις του συστήματος. Η οποιαδήποτε έλλειψη πρέπει να καλύπτεται προτού συνεχιστεί η κατασκευή του συστήματος.

Ο έλεγχος ρεαλισμού πραγματοποιείται ώστε να μπορέσουμε να συμπεράνουμε βάσει υπάρχουσας τεχνολογίας και προϋπολογισμού και ημερομηνία προθεσμίας, αν μπορούμε να φέρουμε εις πέρας την κατασκευή του εν λόγω συστήματος. Αν κάποιο κριτήριο δεν πληρείται, οφείλουμε να ενημερώσουμε τα ενδιαφερόμενα μέρη και να προβούμε σε συζητήσεις προς μορφοποίηση τους. Αυτή η προσέγγιση μπορεί να λειτουργήσει σχετικά αναίμακτα και ανώδυνα, αν το πρόβλημα εμφανίζεται στον προϋπολογισμό ή στην ημερομηνία παράδοσης του συστήματος. Τα πράγματα περιπλέκονται σε περίπτωση που το πρόβλημα εμφανίζεται στον τεχνολογικό τομέα, καθώς μπορεί η τεχνολογία να μην υπάρχει ή να μην την κατέχουμε και να πρέπει να την εισάγουμε από κάποιο τρίτο πρόσωπο.

Η διαδικασία της επαλήθευσης γίνεται ξεκάθαρα ώστε να μην υπάρχει περιθώριο αμφισβήτησης ανάμεσα σε εργολάβο και πελάτη, όσον αφορά τις απαιτήσεις του συστήματος. Ο εργολάβος καθορίζει ορισμένα τεστ τα οποία εφόσον εγκριθούν από τον πελάτη, θα πρέπει κατά την πραγματοποίησή τους να επαληθεύουν τις καταγεγραμμένες απαιτήσεις του συστήματος.


Ανάλυση σκοπιμότητας
Ανάλυση απαιτήσεων
Προσδιορισμός απαιτήσεων
Επικύρωση απαιτήσεων

Κεφάλαιο 3

Διαχείριση κινδύνου

3.1 Εισαγωγή

Ο κίνδυνος είναι η μετρική με την οποία μπορούμε να υπολογίσουμε κατά πόσο απειλείται ένα αγαθό από πιθανές καταστάσεις ή γεγονότα. Υπολογίζεται συναρτήσει των διάφορων επιπτώσεων που μπορεί να επιφέρει ένα συμβάν και την πιθανότητα να συμβεί κάποιο συμβάν. Στα πληροφοριακά συστήματα, ο κίνδυνος είναι παράγωγο της απώλειας της ακεραιότητας, της εμπιστευτικότητας ή της διαθεσιμότητας πληροφοριών ή υπηρεσιών και αντικατοπτρίζει τις πιθανές επιπτώσεις που μπορεί να υποστεί μία εταιρία.

Η απώλεια των ιδιοτήτων ασφαλείας απαιτεί την ύπαρξη τριών διαφορετικών στοιχείων για να συμβεί. Πρέπει να έχουμε ένα αγαθό, μία απειλή και μία ευπάθεια. Αν κάποιο από τα τρία αυτά στοιχεία δεν υφίσταται στο σύστημά μας, τότε μπορούμε να αποφανθούμε πως ο κίνδυνος για το σύστημά μας είναι μηδενικός. Αν δούμε τον κίνδυνο ως συνάρτηση μπορούμε να πούμε πως είναι γινόμενο αυτής της τριάδας.

$$Κίνδυνος = Απειλή \times Ευπάθεια \times Αγαθό$$

Ως απειλή ορίζεται οτιδήποτε μπορεί να εκμεταλλευτεί κάποια αδυναμία του συστήματος με αποτέλεσμα να φέρει στην κατοχή του το αγαθό, να του προκαλέσει ζημιά ή να το καταστρέψει εντελώς. Η ευπάθεια είναι οποιαδήποτε αδυναμία ή κενό των προστατευτικών μας μέσων τα οποία μπορούν να εκμεταλλευθούν τυχόν απειλές. Τέλος, ως αγαθό ορίζουμε οτιδήποτε αξίας το οποίο επιθυμούμε να προστατέψουμε.

Για να κατανοήσετε καλύτερα αυτή την εξίσωση αναλογιστείτε ένα νησί στην μέση του πουθενά. Πάνω σε αυτό το νησί υπάρχει ένα σπίτι με έναν πανάκριβο πίνακα και μία συμμορία ληστών η οποία μόλις κατέφθασε με ένα φουσκωτό. Η συμμορία των ληστών αποτελεί μία ξεκάθαρη απειλή για τον πανάκριβο πίνακα ο οποίος και αποτελεί το αγαθό στο παράδειγμά μας. Εμείς ως ιδιοκτήτες του πίνακα επιθυμούμε να τον προστατέψουμε και βάζουμε στο σπίτι που στεγάζει τον πίνακα πόρτες τελευταίας τεχνολογίας. Αυτές αποτελούν τα μέτρα ασφαλείας που λαμβάνουμε για να μειώσουμε τις πιθανότητες ο πίνακας να κλαπεί.

Σχόλιο [s6]: Πρόσεχα στο μάθημα.

Υπάρχουν τρεις διαφορετικοί τρόποι να τα επίπεδα κινδύνου να φθάσουν σε μηδενικά επίπεδα όπως προαναφέραμε. Μπορούμε να φροντίσουμε να μην υπάρχουν ληστές εξ ορισμού, δηλαδή να μην σκεφτόντουσαν καν να έρθουν στο νησί μας. Κάτι τέτοιο δεν γίνεται στην πραγματικότητα καθώς όλα τα πληροφοριακά συστήματα έχουν απειλές, άλλα μικρές και άλλα μεγαλύτερες. Η δεύτερη σκέψη που κάνουμε είναι να εκμηδενίσουμε το αγαθό. Οι ληστές μπαίνουν στο σπίτι, αλλά ο πίνακας δεν υπάρχει και συνεπώς δεν αποτελούν απειλή για αυτόν.

Όπως μπορείτε να καταλάβετε, όλες μας οι ελπίδες για μηδενισμό του κινδύνου στρέφονται στην καταπολέμηση των ευπαθειών, δηλαδή στην εγκατάσταση μέτρων ασφαλείας. Έτσι θα μπορούμε να έχουμε έναν πανάκριβο πίνακα μέσα στο σπίτι και ακόμα κι αν εμφανιστούν ληστές, δεν θα μπορούν να προκαλέσουν την οποιαδήποτε ζημιά, οπότε είμαστε ασφαλείς. Σε αυτό ακριβώς εδώ το σημείο είναι η μεγαλύτερη παγίδα για οποιοδήποτε εισέρχεται για πρώτη φορά στον κόσμο της διαχείρισης κινδύνου. Τα μέσα ασφαλείας κοστίζουν και πρέπει να ακολουθήσουμε μία αρχή.

Πρόκειται περί οικονομικού λάθους να ξοδεύουμε περισσότερα χρήματα για την προστασία ενός αγαθού, από όσα αξίζει.

Όσο ακριβός και να είναι ο πίνακας, τα δυνητικά προστατευτικά μέτρα μπορούν να κοστίσουν περισσότερο. Μπορούμε να βάλουμε πόρτες ασφαλείας και παράθυρα ασφαλείας. Επίσης μπορούμε να βάλουμε τον πίνακα σε ένα χρηματοκιβώτιο και να εισηγηθούμε το χρηματοκιβώτιο να κρυφτεί σε ειδικό χώρο υπογείως του σπιτιού. Έτσι σίγουρα μειώνουμε τον κίνδυνο καταπολεμώντας τις ευπάθειες ασφαλείας που έχει ο πίνακας, δεν εξαλείφουμε όμως και την απειλή η οποία είναι οι ληστές. Μία καλή ομάδα ληστών με τα κατάλληλα μέσα θα καταφέρει να αποσπάσει από την κατοχή μας αν οι συνθήκες τους ευνοήσουν.

Έχοντας λάβει τα κατάλληλα μέτρα προστασίας και έχοντας μείνει εντός προϋπολογισμού, υπολογίζουμε ξανά τα επίπεδα κινδύνου. Το παράγωγο αυτής της διαδικασίας ονομάζεται πλέον εναπομείναν κίνδυνος. Ο εναπομείναν κίνδυνος χωρίζεται σε πέντε διαφορετικούς τύπους κινδύνου. (8)

Ο πρώτος κίνδυνος που θα εξετάσουμε είναι ο αποδεκτός κίνδυνος. Ως αποδεκτό κίνδυνο μπορούμε να χαρακτηρίσουμε τον κίνδυνο ο οποίος είναι ανάξιος αντιμετώπισης ή απλούστατα δεν μπορούμε να τον αντιμετωπίσουμε με τον δεδομένο προϋπολογισμό. Παράδειγμα αποδεκτού κινδύνου

Ο ελεγχόμενος κίνδυνος παρόλο το όνομά του, παραμένει κίνδυνος. Ως ελεγχόμενους κινδύνους χαρακτηρίζουμε αυτούς για τους οποίους έχουμε λάβει μέτρα ασφαλείας, αλλά δεν έχουμε καταφέρει να τους εξαλείψουμε εντελώς. Παράδειγμα ελεγχόμενου κινδύνου μπορεί να αποτελέσει η απενεργοποίηση του firewall για ορισμένο χρονικό διάστημα ή ένα μη πλήρως ενημερωμένο λογισμικό προστασίας από ιομορφικό λογισμικό.

Ως εξαλειφόμενο κίνδυνο χαρακτηρίζουμε τον κίνδυνο ο οποίος δεν υπολογίζεται πλέον καθώς τα μέσα προστασίας που έχουν εφαρμοστεί έχουν φροντίσει να φτάσει σε μηδενικά επίπεδα. Ένας παρωχημένος ιός δεν αποτελεί πλέον απειλή όταν έρχεται αντιμέτωπος με ένα σύγχρονο λογισμικό καταπολέμησης ιομορφικού λογισμικού.

Ο αποφευγμένος κίνδυνος επίσης δεν αποτελεί πλέον κίνδυνο για το σύστημά μας, αλλά αυτό το αποτέλεσμα δεν επήλθε ως αποτέλεσμα δικών μας πράξεων ή ενεργειών. Για παράδειγμα, τα τείχη προστασίας των παρόχων Διαδικτύου μπορεί να απέτρεψαν επίθεση η οποία απευθυνόταν στο σύστημά μας, παρόλο που εμείς μπορεί να μην το έχουμε ζητήσει.

Το τελευταίο είδος εναπομείναντος κινδύνου είναι ο μεταφερόμενος κίνδυνος. Ο μεταφερόμενος κίνδυνος είναι οποιοσδήποτε κίνδυνος έχουμε φροντίσει να αναληφθεί από κάποιον άλλο η αντιμετώπισή του. Σε περίπτωση που δεν έχουμε την δυνατότητα να αντιμετωπίσουμε πλήρως κάποιο κίνδυνο, έχουμε την επιλογή να τον μεταφέρουμε υπό την δικαιοδοσία κάποιου παρόχου προστατευτικών μέτρων. Η ασφάλιση και η σύναψη συμβολαίων με εταιρίες παρακολούθησης (monitoring) αποτελούν δύο από τις ενέργειες που μπορούμε να πραγματοποιήσουμε, αν θέλουμε να μεταφέρουμε τον κίνδυνο εκτός του συστήματός μας. Ο μεταφερόμενος κίνδυνος παραμένει κίνδυνος, όμως σε περίπτωση συμβάντος, τις επιπτώσεις επιβαρύνει ως επί το πλείστων την οντότητα στην οποία έχουμε μεταφέρει τον κίνδυνο.

3.2 Κατηγορίες κινδύνου

Οι διάφοροι οργανισμοί εκτίθενται σε διάφορους τύπους επιχειρηματικών κινδύνων. Αυτοί οι κίνδυνοι μπορούν να κατηγοριοποιηθούν με μία πλειάδα τρόπων. Παρόλη την κατηγοριοποίηση των

κινδύνων, ένας οργανισμός πρέπει να είναι σε θέση να αντιμετωπίσει πάσης φύσεως κινδύνους, ασχέτως τον τρόπο με τον οποίο τον χαρακτηρίζουμε. (9)

Η πρώτη κατηγορία που θα εξετάσουμε είναι ο οικονομικός κίνδυνος και τον εξετάζουμε πρώτο για ευνόητους λόγους. Στον οικονομικό κόσμο, ο κίνδυνος δεν είναι μία απλή αφαιρετική έννοια χωρίς υπόσταση ή πιθανότητα εμφάνισης. Σε οικονομικούς όρους, ο κίνδυνος είναι η πιθανότητα η πραγματική τιμή επιστροφής μίας επένδυσης να διαφέρει από την αναμενόμενη.

Ο επιχειρησιακός κίνδυνος εγείρεται από την εκτέλεση επιχειρηματικών διαδικασιών και υφίσταται σε επιχειρήσεις οποιουδήποτε μεγέθους. Είναι ένας πολύ ευρύς όρος ο οποίος καλύπτει υπό την ομπρέλα του έννοιες όπως ο κίνδυνος φυσικής ασφάλειας και δημόσιας υγείας, ο φυσικός κίνδυνος, ο κίνδυνος εξαπάτησης, ο κίνδυνος ανθρώπινου δυναμικού και ο κίνδυνος εξωτερικής ανάθεσης καθηκόντων

Η επόμενη κατηγορία που θα μελετήσουμε είναι ο στρατηγικός κίνδυνος. Ως στρατηγικός κίνδυνος μπορεί να χαρακτηριστεί οποιαδήποτε άμεση ή μελλοντική επίπτωση μπορεί να επιφέρουν οι επιχειρηματικές αποφάσεις μίας επιχείρησης, η ακατάλληλη ή ανολοκλήρωτη εφαρμογή αυτών των αποφάσεων αλλά ακόμα και η ακαμψία της επιχείρησης ως προς τις αλλαγές πλεύσης της βιομηχανίας της οποίας είναι μέρος.

Ο κίνδυνος φήμης ανήκει στους τύπους κινδύνου που μπορούν να βλάψουν έναν οργανισμό στο άμεσο μέλλον. Ως κίνδυνο φήμης χαρακτηρίζουμε την οποιαδήποτε αρνητική επίπτωση στο κεφάλαιο και τα κέρδη του οργανισμού, ως αποτέλεσμα της αρνητικής εντύπωσης που μπορεί να έχει μερίδιο του αγοραστικού κοινού ως προς τις πολιτικές αλλά και την γενικότερη συμπεριφορά του οργανισμού.

Ένας άλλος κίνδυνος που ελλοχεύει για τους οργανισμούς, είναι ο κίνδυνος που πηγάζει από τα νομικά πλαίσια που περιβάλλουν την λειτουργία τους. Ο όρος που χρησιμοποιείται για να περιγράψει αυτό τον κίνδυνο είναι κίνδυνος συμμόρφωσης. Παλαιότερα εμπεριεχόταν στον επιχειρησιακό κίνδυνο, αλλά εξελίξεις όπως ο Γενικός Κανονισμός Προστασίας Δεδομένων, έχει αναγκάσει διάφορους οργανισμούς να αποσχίσουν τον κίνδυνο συμμόρφωσης από τον επιχειρησιακό. Αυτή η κίνηση αποσκοπεί στο να δοθεί ιδιαίτερη σημασία στον εν λόγω κίνδυνο καθώς οι επιπτώσεις είναι αρκετά σοβαρές για τις επιχειρήσεις που δεν συμμορφώνονται.

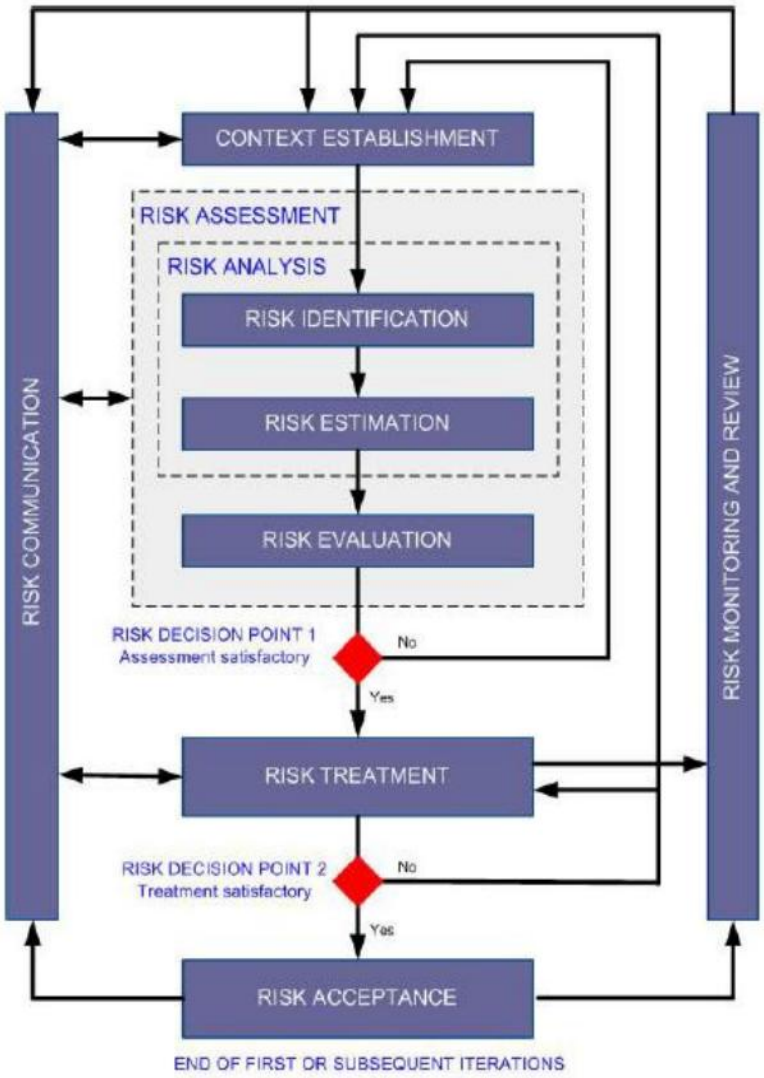
Σχόλιο [s7]: Ξέρω περίεργες λέξεις, μπράβο μου

Το τελευταίο είδος κινδύνου που θα μας απασχολήσει σε αυτή την ενότητα, είναι ο κίνδυνος του πληροφοριακού συστήματος. Ο κίνδυνος του πληροφοριακού συστήματος απορρέει από την οποιαδήποτε επίπτωση μπορεί να επιφέρει η δυσλειτουργία του πληροφοριακού συστήματος στον οργανισμό. Πλέον, λόγω της ανάμιξης του πληροφοριακού συστήματος στην λειτουργία του οργανισμού, αναφερόμαστε σε αυτόν ξεχωριστά και όχι υπό την ομπρέλα του επιχειρησιακού ή στρατηγικού κινδύνου όπως ήταν η βέλτιστη πρακτική τα προηγούμενα χρόνια.

3.3 Διαδικασία διαχείρισης κινδύνου

Για να μπορέσουμε να διαχειριστούμε τον κίνδυνο, είναι αναγκαία η ανάπτυξη μίας διαδικασίας ειδικά σχεδιασμένης για αυτό το σκοπό. Υπάρχουν πολλές μεθοδολογίες και εργαλεία τα οποία υπόσχονται να μας βοηθήσουν να διαχειριστούμε τον κίνδυνο και συνήθως η χρήση τους είναι προτιμότερη από το να προσπαθήσουμε να αναπτύξουμε μία δική μας. Εργαλεία όπως η CRAMM και η EBIOS είναι μερικά από αυτά. Κάνοντας χρήση κάποιου ευρέος διαδεδομένου εργαλείου μπορούμε να είμαστε βέβαιοι για την ποιότητα των αποτελεσμάτων και συνεπώς να αισθανόμαστε περισσότερο ασφαλείς.

Η τυφλή χρήση κάποιου εργαλείου μπορεί να είναι εξίσου επιβλαβής με την δημιουργία κάποιου δικού μας εργαλείου. Για να μπορέσουμε συνεπώς να κατανοήσουμε καλύτερα τα εργαλεία που χρησιμοποιούμε, είναι αναγκαίο να εξετάσουμε τα επί μέρους βήματα που καλύπτει κάθε εργαλείο διαχείρισης κινδύνου ανεξαιρέτως. Προς ευκολότερη κατανόηση του αναγνώστη θα παραθέσουμε μία εικόνα η οποία απεικονίζει κάθε βήμα και κάθε ορισμό της διαδικασίας διαχείρισης κινδύνου. Στην συνέχεια θα επεξηγήσουμε κάθε όρο ξεχωριστά.



ΕΙΚΟΝΑ 2 ΔΙΑΔΙΚΑΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ ΚΙΝΔΥΝΟΥ

Στην παραπάνω εικόνα, μπορούμε να διακρίνουμε πολλούς διαφορετικούς όρους. Στην συνέχεια θα αναφερθούμε στον καθένα ξεχωριστά.

Οι δύο όροι που ξεχωρίζουν κάπως από το παραπάνω σχήμα είναι ο όρος της επικοινωνίας κινδύνου και της επιτήρησης κινδύνου. Αμφότερες οι δύο αυτές διεργασίες, πραγματοποιούνται καθ' όλη την διάρκεια της διαδικασίας διαχείρισης κινδύνου αλλά και μετά το πέρας της όλης διαδικασίας. Εξ ου και ο λόγος που αναπαρίστανται καθ' αυτό τον τρόπο στην παραπάνω εικόνα.

3.3.1 Επικοινωνία κινδύνου

Η επικοινωνία κινδύνου είναι μία περίπλοκη διαδικασία που έχει ως σκοπό να κάνει γνωστό τον τωρινό, τον μελλοντικό αλλά και τον αναδυόμενο κίνδυνο που διατρέχει ένας οργανισμός, στα τυχόν ενδιαφερόμενα μέλη του οργανισμού. Βάσει του μοντέλου CERC (Crisis and Emergency Risk Communication) το οποίο αναπτύχθηκε από το CDC (Center for Disease Control and Prevention), η οποιαδήποτε διαδικασία επικοινωνίας κινδύνου θα πρέπει να έχει τα εξής στοιχεία: (10)

- Αναγνώριση του πιο απαιτητικού κοινού για μηνύματα κινδύνου
- Ανάπτυξη κατάλληλων μηνυμάτων
- Κατανόηση του τρόπου με τον οποίο το κοινό θα επεξεργαστεί τα μηνύματα
- Ανάπτυξη τρόπου ενσωμάτωσης αποκλινόντων συμπεριφορών στο γενικότερο σχέδιο επικοινωνίας

Η διαδικασία επικοινωνίας μπορεί να χωριστεί και σε διαφορετικά χρονικά πλαίσια. Αναλόγως το πλαίσιο θα είναι και διαφορετικές οι ενέργειες στις οποίες θα προβούμε προς επικοινωνία του κινδύνου.

- Προ κρίσης
- Αρχικού συμβάντος
- Συντήρησης
- Λήξη συμβάντος
- Αξιολόγηση

Κατά την διάρκεια του πρώτου σταδίου, τα μηνύματα τα οποία επικοινωνούμε είναι προειδοποιητικής φύσεως και απευθύνονται σε όλα τα ενδιαφερόμενα μέρη. Τα μηνύματα μπορούν να αφορούν γενικές οδηγίες σε περίπτωση συμβάντος και βέλτιστες πρακτικές προετοιμασίας. Κατά την διάρκεια αυτού του σταδίου οφείλουμε να δοκιμάζουμε την αποτελεσματικότητα της επικοινωνίας με τα ενδιαφερόμενα μέρη, προς εξοικείωση αυτών. Αυτή η διαδικασία οφείλει να είναι συστηματική και διαρκώς εξελισσόμενη και αυτός είναι ο λόγος που η συγκεκριμένη διαδικασία καλύπτει όλο το χρονικό πλαίσιο της διαδικασίας διαχείρισης κινδύνου.

Στο δεύτερο στάδιο, ένα πιθανό συμβάν έχει μόλις εμφανιστεί και ίσως να μην έχει γίνει ακόμα αισθητό από τα ενδιαφερόμενα μέλη. Σκοπός της διαδικασίας είναι να ενημερώσει εγκαίρως για τον κίνδυνο, τις επηρεαζόμενες οντότητες προς μείωση των επιπέδων αβεβαιότητας μεταξύ τους καθώς και αύξηση της αυτό-αποτελεσματικότητας των επόμενων ενεργειών τους.

Το στάδιο συντήρησης έχει ως σκοπό να κρατάει τα ενδιαφερόμενα μέρη ενημερωμένα αλλά και σε επιφυλακή κατά την διάρκεια του συμβάντος. Ταυτοχρόνως οφείλουμε να επεξεργαζόμαστε τυχόν ανατροφοδότηση πληροφορίας από τα ενδιαφερόμενα μέλη και να αντιμετωπίζουμε συμβάντα παραπληροφόρησης τα οποία μπορούν να επηρεάσουν την γενικότερη διαδικασία διαχείρισης κινδύνου.

Όταν ένα συμβάν λήξει, οφείλουμε προφανώς να ενημερώσουμε τα επηρεαζόμενα μέλη. Μέρος της ενημέρωσης αποτελεί η πληροφόρηση ως προς το πως αντιμετωπίστηκε το συμβάν, κατά πόσο

αποτελεσματικός ήταν αυτός ο τρόπος, καθώς επίσης γίνεται και ανασκόπηση τυχόν προβλημάτων τα οποία εμφανίστηκαν κατά την διάρκεια του συμβάντος και επηρέασαν την όλη αποτελεσματικότητα της διαδικασίας διαχείρισης κινδύνου.

Τελικό στάδιο της επικοινωνίας κινδύνου αποτελεί το στάδιο αξιολόγησης. Κατά την διάρκεια αυτού του σταδίου, αξιολογούμε με τις αρμόδιες αρχές κατά πόσο αποτελεσματικοί ήταν οι τρόποι με τους οποίους αντιμετωπίσθηκε το συμβάν και ξεκινούμε μία διαδικασία βελτίωσης των διαδικασιών που χρησιμοποιήθηκαν εφόσον αυτό κριθεί απαραίτητο. Ταυτοχρόνως φροντίζουμε να επανέλθουμε στο αρχικό στάδιο της επικοινωνίας κινδύνου, στο στάδιο προ κρίσης.

3.3.2 Επίβλεψη κινδύνου

Η δεύτερη διαδικασία που πραγματοποιείται καθ' όλη την διάρκεια της διαδικασίας διαχείρισης κινδύνου είναι η επίβλεψη κινδύνου. Η συνεχής επίβλεψη κινδύνου, εξασφαλίζει ότι νέοι και αναδυόμενοι κίνδυνοι ανιχνεύονται εγκαίρως και συμπεριλαμβάνονται στην όλη διαδικασία της διαχείρισης κινδύνου σε οποιοδήποτε στάδιο κι αν βρίσκεται. Πιο συγκεκριμένα, με την διαδικασία επίβλεψης κινδύνου, παρακολουθούμε τους ήδη αναγνωρισμένους κινδύνους, τον εναπομείναν κίνδυνο αλλά και όπως προαναφέραμε τους νέους κινδύνους που εμφανίζονται.

Η λίστα με τους κινδύνους που μπορούν να βλάψουν έναν οργανισμό δεν είναι στατικοί, μεταβάλλεται και εξελίσσεται ακριβώς όπως και οι κίνδυνοι που περιλαμβάνει. Σε αυτό το σημείο να αναφερθούμε στο γεγονός πως ο κίνδυνος δεν μπορεί να αυξηθεί ή να εξελιχθεί, αλλά και να εξαφανιστεί. Ανεξαρτήτως συμπεριφοράς κάποιου κινδύνου, οφείλουμε να τον παρακολουθούμε και να έχουμε πλήρη γνώση της κατάστασής του.

Η συγκεκριμένη διαδικασία συνδέεται και στηρίζεται με την διαδικασία επικοινωνίας κινδύνου. Κάθε αλλαγή που συμβαίνει σε κάποιο κίνδυνο πρέπει να γνωστοποιείται στα κατάλληλα άτομα. Αυτό μπορεί να βοηθήσει στην έγκαιρη αντιμετώπιση ενός κινδύνου ή ακόμα και στην αποφυγή του ολοκληρωτικά.

Όταν η ομάδα που εκτελεί την διαδικασία διαχείρισης κινδύνου ενημερωθεί για την μεταβολή της κατάστασης κάποιου κινδύνου, οφείλει να:

- Αναγνωρίσει, αναλύσει και λάβει τα κατάλληλα αντίμετρα για κάποιον καινούριο κίνδυνο.
- Να πραγματοποιήσει ανασκόπηση των διαδικασιών αντιμετώπισης κινδύνου καθώς μπορεί να έχει επηρεαστεί η αποτελεσματικότητά τους, δεδομένης της μεταβολής κάποιου κινδύνου

Όταν ένας κίνδυνος κηρύσσεται παρωχημένος, η ομάδα που πραγματοποιεί την διαδικασία διαχείρισης κινδύνου πραγματοποιεί ανασκόπηση των διαδικασιών που αφορούσαν τον συγκεκριμένο κίνδυνο και εξετάζει κατά πόσο αποτελεσματικές μπορεί να ήταν σε περίπτωση εμφάνισης πραγματικού συμβάντος ασφαλείας. (11)

3.3.3 Καθιέρωση πλαισίου

Προτού ξεκινήσει η διαδικασία της διαχείρισης κινδύνου είναι αναγκαίο να καθιερωθεί ένα πλαίσιο το οποίο θα μας προσφέρει την κατάλληλη πληροφορία για τον οργανισμό. Έχοντας στην κατοχή μας και επεξεργαζόμενοι τις πληροφορίες που θα αναλύσουμε λίγο παρακάτω, μπορούμε να είμαστε βέβαιοι για την ακρίβεια και την ποιότητα των αποτελεσμάτων της διαδικασίας που θα πραγματοποιήσουμε. Η πληροφορία που χρειαζόμαστε χωρίζεται σε δύο ομάδες. Το εσωτερικό πλαίσιο και το εξωτερικό πλαίσιο.

Στο εξωτερικό πλαίσιο, κατηγοριοποιούμε πληροφορίες όπως:

- Νομικό πλαίσιο
- Κανονιστικό πλαίσιο

- Οικονομικό περιβάλλον
- Τεχνολογικό περιβάλλον
- Περιβάλλον αγοράς
- Εξωτερικά ενδιαφερόμενα μέλη

Καθώς η διαδικασία διαχείρισης κινδύνου λαμβάνει υπόψιν της τους στόχους και τους σκοπούς ενός οργανισμού, κρίνεται αναγκαίο να γνωρίζουμε και το εσωτερικό πλαίσιο. Στο εσωτερικό πλαίσιο ενός οργανισμού, κατηγοριοποιούμε πληροφορία όπως:

- Οργανόγραμμα
- Πολιτικές του οργανισμού
- Σκοπούς οργανισμού
- Στρατηγικές επίτευξης στόχων
- Πόρους
- Πληροφοριακά συστήματα
- Συμβατικές υποχρεώσεις
- Πρότυπα, οδηγίες και μοντέλα τα οποία έχει υιοθετήσει ο οργανισμός

Μόνο μέσω εξονυχιστικής εξέτασης του περιβάλλοντος του οργανισμού μπορούμε να προβούμε σε μία διαδικασία διαχείρισης κινδύνου της οποίας τα αποτελέσματα θα ταιριάζουν και θα επωφελήσουν τον οργανισμό. Σε διαφορετική περίπτωση, κινδυνεύουμε να οδηγηθούμε σε αποτελέσματα τα οποία μπορούν να αποβούν ζημιογόνα στον οργανισμό.

3.3.4 Αναγνώριση κινδύνου

Σε αυτή την φάση της διαδικασίας διαχείρισης κινδύνου γίνεται αναγνώριση των απειλών, των ευπαθειών και των συσχετιζόμενων κινδύνων. Αυτή η διαδικασία ονομάζεται διαδικασία αναγνώρισης κινδύνου. Η διαδικασία αναγνώρισης κινδύνου πρέπει να είναι συστηματική και εξονυχιστική ώστε όλοι οι πιθανοί κίνδυνοι να ληφθούν υπόψη. Ακόμα κι αν ένας κίνδυνος είναι γνωστός στον οργανισμό, οι βέλτιστες πρακτικές σημειώνουν πως είναι αναγκαία η καταγραφή τους.

Πρώτο βήμα αυτής της διαδικασίας είναι η κατασκευή μίας λίστας η οποία θα περιέχει πηγές απειλών, κινδύνους και συμβάντα τα οποία μπορούν να επηρεάσουν αρνητικά τις προσπάθειες ενός οργανισμού να επιτύχουν τους στόχους τους, όπως αυτοί καθορίστηκαν στην προηγούμενη φάση της διαδικασίας διαχείρισης κινδύνου.

Σε αυτό το στάδιο, ένας κίνδυνος μπορεί να χαρακτηρίζεται από:

- Την πηγή του. (Υπάλληλοι του οργανισμού, ανταγωνισμός κλπ.)
- Κάποια συγκεκριμένη δραστηριότητα, συμβάν ή περιστατικό. (Διαρροή δεδομένων, κινήσεις ανταγωνισμού, ενημερώσεις στο νομικό πλαίσιο το οποίο υπάγεται ο οργανισμός κλπ.)
- Τις επιπτώσεις. (Μη διαθεσιμότητα υπηρεσίας, απώλεια κερδών, πρόστιμα κλπ.)
- Προστατευτικούς μηχανισμούς
- Ώρα και μέρος εμφάνισης συμβάντος.

Η πληροφορία που έχουμε εξαγάγει κατά την διάρκεια διαδικασίας καθιέρωσης πλαισίου, έχει κύριο ρόλο και σε αυτή την φάση της διαδικασίας διαχείρισης κινδύνου. Χωρίς αυτή την πληροφορία δεν θα μπορούσαμε να είμαστε σε θέση να αναγνωρίσουμε πιθανούς κινδύνους τους οποίους διατρέχει ο οργανισμός καθώς και να προτείνουμε τους κατάλληλους προστατευτικούς μηχανισμούς. Πληροφορίες επί πιθανών προηγούμενων συμβάντων, μπορούν να βοηθήσουν στην καλύτερη κατανόηση του περιβάλλοντος τους οργανισμού καθώς και στην επιλογή προστατευτικών μηχανισμών.

Το να αναγνωρίζουμε τι μπορεί να συμβεί σπάνια καταλήγει να είναι αρκετό. Το γεγονός ότι ένα συμβάν μπορεί να συμβεί με πολλούς διαφορετικούς τρόπους κάνει αναγκαία την μελέτη όλων των πιθανών σεναρίων και σημαντικών αιτιών τα οποία μπορούν να οδηγήσουν σε ένα συμβάν. Μέθοδοι και εργαλεία όπως ερωτηματολόγια και διαγράμματα ροής είναι στην διάθεση της ομάδας που διεξάγει την διαδικασία αναγνώρισης κινδύνου ώστε να μπορούν να είναι αποτελεσματικότεροι. (12)

3.3.5 Εκτίμηση κινδύνου

Η διαδικασία αναγνώρισης κινδύνου σε συνδυασμό με την διαδικασία εκτίμησης κινδύνου, αποκαλούνται από την βιβλιογραφία ως διαδικασία ανάλυσης κινδύνου. Σε αυτή την ενότητα θα μιλήσουμε για την διαδικασία εκτίμησης κινδύνου συνεχίζοντας την ανάλυση των διαφορετικών διαδικασιών της διαδικασίας διαχείρισης κινδύνου.

Σκοπός αυτής της διαδικασίας είναι η επιλογή κάποιας κλίμακας μέτρησης στην πιθανότητα να συμβεί ένα περιστατικό, καθώς επίσης και στις επιπτώσεις που μπορεί να επιφέρει η εμφάνιση ενός περιστατικού. Η συνηθέστερη κλίμακα χρησιμοποιεί τις λέξεις “High, Medium, Low”. Αν χρειαζόμαστε περισσότερη λεπτομέρεια στην κλίμακα μας, μπορούμε να την επεκτείνουμε προσθέτοντας κατηγορίες όπως “Very High, Very Low, Highest, Minimum”. Η επιλογή κλίμακας είναι στην δική μας ευχέρεια, καθώς επίσης και ο βαθμός λεπτομέρειας ο οποίος θα διαλέξουμε. Οι λέξεις αυτής της κλίμακας δεν αναπαριστούν μόνο την πιθανότητα και τις επιπτώσεις, αλλά θα χρησιμοποιηθούν για να κατηγοριοποιήσουμε τον κίνδυνο.

Έχοντας επιλέξει κλίμακα, κατασκευάζουμε έναν πίνακα ο οποίος θα μας βοηθήσει να υπολογίσουμε τον κίνδυνο. Τοποθετούμε στον άξονα Χ την πιθανότητα να συμβεί ένα συμβάν και στον άξονα Υ τις επιπτώσεις που μπορεί να έχει ένα συμβάν. Αυτό το βήμα είναι τελείως αυθαίρετο και οι 2 άξονες θα μπορούσαν κάλλιστα να είναι αντεστραμμένοι.

Επίπτωση	Critical					
	High					
	Medium					
	Low					
	Minimum					
Πιθανότητα Εμφάνισης		Minimum	Low	Medium	High	Almost Certain

Όπως μπορείτε να δείτε ο πίνακας που παραθέσαμε είναι άδειος. Ο συνδυασμός πιθανότητας εμφάνισης και επίπτωσης πρέπει ως παράγωγο να μας προσφέρει το επίπεδο κινδύνου. Για να γίνει αυτό χρειάζεται να πραγματοποιήσουμε 3 παραπάνω βήματα. Να επιλέξουμε ένα μαθηματικό μοντέλο υπολογισμού και να ορίσουμε τα επίπεδα κινδύνου τα οποία θα έχουμε. Για να ταιριάξουν οι κλίμακες που έχουμε αποδώσει, στο μαθηματικό μοντέλο πρέπει να τις συνδέσουμε με έναν αριθμό.

Στην δική μας περίπτωση, το μαθηματικό μοντέλο θα είναι ο πολλαπλασιασμός και για να πραγματοποιήσουμε πολλαπλασιασμό θα αποδώσουμε τις παρακάτω τιμές στην κλίμακά μας.

Επίπτωση	
Critical	5
High	4
Medium	3
Low	2

Minimum	1

Πιθανότητα εμφάνισης	
Almost Certain	5
High	4
Medium	3
Low	2
Minimum	1

Έχοντας κατασκευάσει τους παραπάνω πίνακες χρειάζεται να αποφασίσουμε πόσες βαθμίδες θα έχει ο κίνδυνος στο μοντέλο μας και ποιες θα είναι οι τιμές που θα αποδώσουμε στην κάθε βαθμίδα. Εμείς σε αυτή την πτυχιακή εργασία, θα επιλέξουμε το μοντέλο κινδύνου μας να έχει 3 βαθμίδες, High, Medium, Low οι βαθμίδες θα κατανέμονται ως εξής.

Κίνδυνος	
High	>14 (15-25)
Medium	>3 & <15 (4-14)
Low	<4 (0-3)

Εφόσον έχουμε συλλέξει τις παραπάνω πληροφορίες, είμαστε έτοιμοι να συμπληρώσουμε τον πίνακα κινδύνου.

Επίπτωση	Critical	5	10	15	20	25
	High	4	8	12	16	20
	Medium	3	6	9	12	15
	Low	2	4	6	8	10
	Minimum	1	2	3	4	5
Πιθανότητα Εμφάνισης		Minimum	Low	Medium	High	Almost Certain

Με πράσινο χρώμα αποδώσαμε τον κίνδυνο κατηγορίας Low, με κίτρινο αποδώσαμε τον κίνδυνο κατηγορίας Medium και με κόκκινο αποδώσαμε τον κίνδυνο κατηγορίας High.

Όλες οι τιμές καθώς και το μαθηματικό μοντέλο που επιλέξαμε δεν είναι απόλυτες. Τα πάντα μπορούν να αλλάξουν ώστε να ταιριάξουν καλύτερα στην οντότητα πάνω στην οποία θα εφαρμοστεί, είτε αυτή είναι ένας ολόκληρος οργανισμός, είτε αυτή είναι ένα project.

3.3.6 Αξιολόγηση κινδύνου

Θα έλεγε κανείς πως έχοντας δημιουργήσει τόσους πίνακες θα ήμασταν έτοιμοι να προχωρήσουμε στο στάδιο επιλογής μέτρων προς αντιμετώπιση των κινδύνων. Εγείρεται όμως το εξής πρόβλημα. Μιας και η διαδικασία διαχείρισης κινδύνου είναι μια διαδικασία η οποία γίνεται ανά τακτά χρονικά διαστήματα, πρέπει τα αποτελέσματά της, δεδομένου ότι έχουμε τις ίδιες παραμέτρους, να βγαίνουν ίδια κάθε φορά.

Αυτό όπως μπορείτε να φανταστείτε δεν συμβαίνει. Όπως είδαμε και στην προηγούμενη ενότητα όταν προσπαθούμε να χαρακτηρίσουμε έναν κίνδυνο χρειαζόμαστε δύο παραμέτρους. Την

πιθανότητα και τη επίπτωση. Η πιθανότητα να συμβεί ένα συμβάν μπορεί να εξαχθεί μελετώντας στοιχεία που αφορούν παράγοντες του συμβάντος. Για παράδειγμα αν κάποιος κίνδυνος έχει ως πηγή τον σκληρό δίσκο, μπορούμε να υπολογίσουμε την πιθανότητα του να χαλάσει χρησιμοποιώντας στοιχεία όπως τον MTBF χρόνο, τον φόρτο εργασίας του ή την εγγύηση που προσφέρει ο κατασκευαστής. Αν θέλουμε να υπολογίσουμε πόσο πιθανό είναι να πληγεί κάποιο data center μας από τσουνάμι, μπορούμε να χρησιμοποιήσουμε στοιχεία όπως την σεισμική δραστηριότητα της περιοχής και τα γεωγραφικά χαρακτηριστικά της. Με τον ένα ή με τον άλλο τρόπο η πιθανότητα να συμβεί ένα συμβάν μπορεί να υπολογιστεί. Επίσης μπορούμε να είμαστε βέβαιοι πως κάθε φορά που θα πραγματοποιούμε την ίδια διαδικασία, θα ακολουθούμε την ίδια διαδικασία υπολογισμού και συνεπώς τα αποτελέσματά μας μπορούν να θεωρούνται έγκαιρα.

Ο υπολογισμός επίπτωσης όμως παραμένει αυθαίρετος. Χρειαζόμαστε έναν μηχανισμό ο οποίος θα εξασφαλίζει πως ο υπολογισμός επίπτωσης θα είναι έγκυρος και κάθε φορά που θα πραγματοποιείται τα αποτελέσματά του θα είναι υπολογισμένα βάσει προκαθορισμένων κριτηρίων. Αυτό που μπορούμε να κάνουμε είναι να κατασκευάσουμε έναν πίνακα ο οποίος θα προσδιορίζει αυτά τα κριτήρια. Η επιλογή κριτηρίων δεν είναι απόλυτη και συνήθως καθορίζονται από τον οργανισμό. Μπορεί να είναι το οικονομικό κόστος, το κόστος σε ανθρώπινες ζωές ή το κόστος σε χρόνο. Μπορούμε να έχουμε και πολλαπλά κριτήρια, η επιλογή ενός κριτηρίου δεν είναι υποχρεωτική. Για παράδειγμα μπορούμε να διαλέξουμε να υπολογίσουμε την επίπτωση κάποιου συμβάντος βάσει των χρημάτων που θα μας κοστίσει και να υπολογίσουμε την επίπτωση κάποιου άλλου συμβάντος βάσει του χρόνου που θα μας κοστίσει. Εφόσον έχουμε θέσει αυτά τα κριτήρια μπορούμε να είμαστε σίγουροι πως η τακτική εκτέλεση αυτής της διαδικασίας θα αποφέρει έγκυρα αποτελέσματα.

Ας πάρουμε για παράδειγμα ένα μοντέλο υπολογισμού επίπτωσης βάσει οικονομικού κόστους. Για να υιοθετήσουμε ένα τέτοιο μοντέλο, χρειάζεται να κατασκευάσουμε έναν πίνακα στον οποίο θα αντιστοιχίζεται μία βαθμίδα κινδύνου με κάποιο οικονομικό κόστος. Οι τιμές της κλίμακας οικονομικού κόστους είναι μεταβλητές και καθορίζονται βάσει οργανισμού. Για παράδειγμα η απώλεια 10.000 ευρώ σε ένα περίπτερο δεν έχει την ίδια βαρύτητα με την απώλεια του ίδιου ποσού από μία εταιρία όπως η Google για παράδειγμα. Συνεχίζοντας το παράδειγμα των προηγούμενων ενοτήτων, κατασκευάζουμε τον παρακάτω πίνακα χρησιμοποιώντας ένα οικονομικό κριτήριο.

Οικονομικό κόστος	Βαθμός επίπτωσης
<10.000	1
=>10.000 && <20.000	2
=> 20.000 && <50.000	3
=>50.000 && < 100.000	4
=> 100.000	5

Όπως προαναφέρθηκε, ο παραπάνω πίνακας είναι ενδεικτικός. Θα πρέπει να κατασκευάζεται ξεχωριστός πίνακας ο οποίος θα λαμβάνει υπόψη τους στόχους και τους σκοπούς του οργανισμού.

3.3.7 Αντιμετώπιση κινδύνου

Σύμφωνα με το (13), η αντιμετώπιση κινδύνου είναι η διαδικασία κατά την οποία επιλέγουμε και εφαρμόζουμε μέτρα προς αντιμετώπιση του κινδύνου. Τα μέτρα μπορούν να κατηγοριοποιηθούν σε τέσσερις διαφορετικές κατηγορίες· αποφυγή, βελτιστοποίηση, μεταφορά και διατήρηση. Τα μέτρα πρέπει να επιλεχθούν έτσι ώστε να υποστηρίζονται από το πλαίσιο και τις πολιτικές ασφαλείας του οργανισμού που επιθυμεί να τα εφαρμόσει. Στον χώρο της διαχείρισης κινδύνου, τα μέτρα είναι

γραπτές περιγραφές των μέτρων και των διαφόρων λειτουργιών ασφαλείας που μπορούν να προσφέρουν. Μπορούμε να τα διαχωρίσουμε σε δύο διαφορετικές κατηγορίες, τα τεχνικά και τα διαδικαστικά μέτρα.

Συνεχίζοντας την διαδικασία διαχείρισης κινδύνου και έχοντας διαθέσιμα τα αποτελέσματα των προηγούμενων φάσεων της διαδικασίας διαχείρισης κινδύνου, αναγνωρίζουμε της κατάλληλες πράξεις στις οποίες μπορούμε να προβούμε προς διαχείριση του κινδύνου και πως αυτά επηρεάζουν τα επίπεδα κινδύνου αφότου εφαρμοστούν.

Οι αναγνωρισμένο κίνδυνοι οι οποίοι θα έχουν κάποια επίπτωση στον οργανισμό, δεν είναι απαραίτητο πως θα έχουν απαραίτητα κακό αποτέλεσμα. Από κάποιους κινδύνους μπορούν να εγερθούν και ευκαιρίες για τον οργανισμό. Έτσι διαχωρίζουμε τα μέτρα βάσει των αρνητικών και των θετικών αποτελεσμάτων που θα έχουν. Στα διαφορετικά μέτρα που μπορούμε να λάβουμε, αναγνωρίζονται τα εξής θετικά αποτελέσματα:

- Εκκίνηση δραστηριότητας η οποία πιθανώς να δημιουργήσει ή να διατηρήσει κάποιο θετικό αποτέλεσμα.
- Τροποποίηση των επιπέδων εμφάνισης του κινδύνου, προς αύξηση θετικών αποτελεσμάτων.
- Τροποποίηση των επιπέδων των επιπτώσεων του κινδύνου, προς αύξηση αναμενόμενων κερδών.
- Διαμοιρασμός του κινδύνου, με απώτερο σκοπό την κοινή χρήση πόρων σε περίπτωση εμφάνισης περιστατικού.
- Διατήρηση του εναπομείναντος κινδύνου.

Στην αντίπερα όχθη, στα μέτρα που επηρεάζουν τα αρνητικά αποτελέσματα ενός κινδύνου, αναγνωρίζονται τα εξής:

- Προς αποφυγή του κινδύνου, αναβολή της δραστηριότητας που τον προκαλεί.
- Τροποποίηση των επιπέδων πιθανότητας εμφάνισης κινδύνου που προσπαθεί να μειώσει ή να εξαλείψει την πιθανότητα αρνητικών αποτελεσμάτων.
- Τροποποίηση της πιθανότητας εμφάνισης συμβάντος με τέτοιο τρόπο που να οδηγεί σε μείωση χαμένων πόρων.
- Διαμοιρασμός του κινδύνου με οντότητες που αντιμετωπίζουν τον ίδιο κίνδυνο.

Γενικά, το κόστος διαχείρισης του κινδύνου θα πρέπει να συγκρίνεται με τα πλεονεκτήματα τα οποία προσφέρει. Κατά την φάση της ανασκόπησης της διαδικασίας διαχείρισης κινδύνου θα πρέπει να λαμβάνεται υπόψη το περιβάλλον του οργανισμού ώστε να ξέρουμε αν τα μέτρα που επιλέξαμε είναι οικονομικώς βιώσιμα για τον οργανισμό που τα εφαρμόζει. Σε περίπτωση που οι πόροι δεν είναι αρκετοί, ένα πλάνο δράσης θα πρέπει να καθορίζει μία σειρά προτεραιότητας κινδύνου, να αποδίδει βάρη σε κινδύνους ίδιας κλίμακας ώστε να καθορίζεται η σειρά με την οποία θα εφαρμόζονται τα μέτρα.

3.3.8 Πλάνο δράσης διαχείρισης κινδύνου

Το πλάνο δράσης περιέχει επίσης και τις οδηγίες οι οποίες θα βοηθήσουν τον οργανισμό να εφαρμόσει τα μέτρα ασφαλείας που επιλέχθηκαν στην προηγούμενη φάση. Θα πρέπει να είναι αναλυτικά και να περιέχουν όλη την απαραίτητη πληροφορία σχετικά με:

- Προτεινόμενες δράσεις, προτεραιότητες και χρονικά διαγράμματα.
- Πόρους απαιτήσεων.
- Ρόλους και ευθύνες όλων των εμπλεκομένων μερών των προτεινόμενων δράσεων.
- Μετρικές απόδοσης.

- Απαιτήσεις επίβλεψης και αναφοράς.

Το πλάνο δράσης θα πρέπει να αντικατοπτρίζει της οπτικές γωνίες και τις αξίες των εμπλεκομένων μερών και των διάφορων ενδιαφερόμενων μερών. Όσο πιο πολύ συγκλίνουν τα αποτελέσματα των μέτρων ασφαλείας, με τους στόχους και τον τρόπο επίτευξης των στόχων των παραπάνω, τόσο πιο πιθανό είναι να εγκριθούν τα μέτρα και να αρχίσει η διαδικασία εφαρμογής τους. Όπως και με όλες τις σχετικές διαχειριστικές διαδικασίες, η αρχική έγκριση δεν είναι αρκετή ώστε να διασφαλιστεί η αποδοτική εφαρμογή της. Η στήριξη της διοίκησης είναι αναγκαία καθ' όλη την διάρκεια της διαδικασίας. Για αυτό τον λόγο είναι ευθύνη του ιδιοκτήτη της διαδικασίας διαχείρισης κινδύνου να διατηρεί την διοίκηση σε συνεχή και έγκυρη ενημέρωση.

Το πλάνο δράσης θα πρέπει να ορίζει επίσης τον τρόπο με τον οποίο θα εφαρμοστούν τα μέτρα της διαδικασίας διαχείρισης κινδύνου καθ' όλη την έκταση του οργανισμού. Θα πρέπει να κατασκευαστεί με τρόπο ο οποίος θα εξασφαλίζει ότι τα μέτρα θα ενσωματώνεται με τις ήδη υπάρχουσες διαδικασίες του οργανισμού. Αυτή η ενσωμάτωση θα πρέπει να γίνεται με τρόπο ο οποίος θα εξασφαλίζει ότι η εφαρμογή των μέτρων θα είναι σχετική με τις επηρεαζόμενες διαδικασίες και δεν θα επηρεάζει αρνητικά την αποδοτικότητά τους.

Πιο συγκεκριμένα, η διαδικασία διαχείρισης κινδύνου θα πρέπει να ενσωματωθεί στην διαδικασία κατασκευής πολιτικών του οργανισμού, στον επιχειρηματικό και στρατηγικό σχεδιασμό του οργανισμού και στην διαδικασία αλλαγής διαχείρισης. Είναι επίσης πιθανό να ενσωματωθεί σε άλλα σχέδια ή διαδικασίες του οργανισμού όπως στην διαχείριση περιουσιακών στοιχείων του οργανισμού, τις επιθεωρήσεις, τα σχέδια επιχειρηματικής συνέχειας, την περιβαλλοντική πολιτική, τον έλεγχο απατών, το τμήμα ανθρώπινου δυναμικού, καθώς και τα τμήματα επενδύσεων και διαχείρισης νέων μελετών.

Η απαραίτητη επίγνωση και δέσμευση των ανώτερων διοικητικών επιπέδων προς την διαχείριση κινδύνου είναι ύψιστης σημασίας και θα πρέπει να περιλαμβάνει τα εξής στοιχεία:

- Ενεργή υποστήριξη προς την ανάπτυξη και εφαρμογή του σχεδίου.
- Διορισμό υπευθύνου προς ηγεσία και υποστήριξη πρωτοβουλιών.
- Ενεργή υποστήριξη όλων των υπευθύνων διαφορετικών τμημάτων.

Το διοικητικό συμβούλιο του οργανισμού θα πρέπει να ορίσει και να καταγράψει την πολιτική του οργανισμού σε σχέση με την διαχείριση κινδύνου, συμπεριλαμβάνοντας τους στόχους και μία δήλωση δέσμευσης προς την διαδικασία διαχείρισης κινδύνου. Αυτή η πολιτική μπορεί να περιέχει τα εξής στοιχεία:

- Τους στόχους στους οποίου αποσκοπεί η διαχείριση κινδύνου και ποιο το σκεπτικό πίσω από αυτή την πορεία δράσης.
- Την σύνδεση μεταξύ πολιτικής και στρατηγικών πλάνων του οργανισμού.
- Το εύρος της διαδικασίας διαχείρισης κινδύνου.
- Τις διαδικασίες που θα χρησιμοποιηθούν ώστε να πραγματοποιηθεί η διαχείριση κινδύνου.
- Ανάθεση ευθυνών για συγκεκριμένους κινδύνους.
- Λεπτομέρειες διαθέσιμης υποστήριξης όσων διαχειρίζονται κινδύνους.
- Τον τρόπο με τον οποίο θα γίνεται η μέτρηση αποδοτικότητας του σχεδίου και πως αυτή θα αναφέρεται στον οργανισμό.
- Δήλωση δέσμευσης στην τακτή ανασκόπηση της διαδικασίας διαχείρισης κινδύνου.
- Δήλωση δέσμευσης στην πολιτική από το διοικητικό συμβούλιο και τα ανώτερα στελέχη του οργανισμού.

Η δημοσίευση και επικοινωνία μίας πολιτικής τέτοιου είδους, επιδεικνύει τις προθέσεις του οργανισμού στο εσωτερικό και εξωτερικό του περιβάλλον και ορίζονται ξεκάθαρα οι όποιες ευθύνες στα κατάλληλα στελέχη του οργανισμού. Το διοικητικό συμβούλιο και τα ανώτερα διοικητικά στελέχη είναι τα άτομα τα οποία ουσιαστικά είναι υπεύθυνοι για την διαχείριση του κινδύνου στον οργανισμό. Όλο το προσωπικό όμως είναι υπεύθυνο για την διαχείριση κινδύνων στην περιοχή του οργανισμού στην οποία ανήκουν. Ορισμένες κινήσεις που μπορούμε να κάνουμε ώστε να γίνει ευκολότερη η απόδοση ευθυνών είναι οι εξής:

- Προσδιορισμός υπευθύνων προς διαχείριση ορισμένων κινδύνων, εφαρμογή των μέτρων και συντήρηση αυτών.
- Καθορισμός μετρικών απόδοσης και διαδικασιών αναφοράς
- Εξασφάλιση των κατάλληλων επιπέδων αναγνώρισης, ανταμοιβής, έγκρισης αλλά και κυρώσεων

Μέχρι αυτό το σημείο πιστεύουμε πως έχει γίνει προφανές πως η πραγματική εφαρμογή μέτρων ασφαλείας για το πληροφοριακό σύστημα δεν είναι μέρος της διαδικασίας διαχείρισης κινδύνου. Τα μέτρα θα εφαρμοστούν από το κατάλληλο ανθρώπινο δυναμικό με σκοπό την μείωση του κινδύνου.

3.4 Η μέθοδος EBIOS

Η Γαλλικής προελεύσεως μεθοδολογία διαχείρισης κινδύνου EBIOS (Expression des Besoins et Identification des Objectifs de Securite - Expression of Needs and Identification of Security Objectives) χρησιμοποιείται προς εκτίμηση κινδύνου που αφορά την ασφάλεια των πληροφοριακών συστημάτων. Μπορεί επίσης να χρησιμοποιηθεί προς επικοινωνία της όλης διαδικασίας στον οργανισμό αλλά και στους συνεργάτες, συνεπώς συμβάλλει στην διαδικασία διαχείρισης κινδύνου.

Παρέχοντας πληροφορία για την διαδικασία διαχείρισης κινδύνου, αποτελεί ένα αξιόλογο εργαλείο το οποίο υποστηρίζει την λήψη αποφάσεων που σχετίζεται με τα περιουσιακά στοιχεία του οργανισμού, ενημερώνει για τις επιπτώσεις των κινδύνων στον οργανισμό και βοηθά στην αναγνώριση των στόχων ασφαλείας από το περιβάλλον του οργανισμού. Επίσης παρέχει ένα εξαιρετικό πλαίσιο επίγνωσης του κινδύνου για όλους όσους εμπλέκονται με τον οργανισμό (ανώτερα διοικητικά μέλη, ανώτερα στελέχη του οργανισμού, αλλά και εξωτερικούς συνεργάτες), αυξάνοντας την γνώση τους πάνω στην ασφάλεια των πληροφοριακών συστημάτων του οργανισμού.

Μπορεί να χρησιμοποιηθεί για πολλούς διαφορετικούς σκοπούς και πρωτοβουλίες ασφαλείας όπως την δημιουργία κύριου πλάνου ασφαλείας του πληροφοριακού συστήματος, την δημιουργία της πολιτικής ασφαλείας του οργανισμού αλλά και να βοηθήσει στην προετοιμασία του οργανισμού προς πλήρωση απαιτήσεων και standards μηχανισμών όπως το ISO:27001. Βέλτιστη χρονική περίοδος χρήσης της μεθοδολογίας είναι κατά την αρχική φάση σχεδίασης ενός πληροφοριακού συστήματος. Κατά την διάρκεια αυτής της φάσης, οι πρακτικές της μεθοδολογίας μπορούν να ενσωματωθούν στις διαδικασίες του πληροφοριακού συστήματος, κάνοντας την συμβίωση του πληροφοριακού συστήματος με τις πρακτικές που θα προτείνει η EBIOS αδιάλειπτη. Εάν το πληροφοριακό σύστημα έχει κατασκευαστεί χωρίς την EBIOS, η μεθοδολογία θα λάβει υπόψη της τα υπάρχοντα μέτρα ασφαλείας και θα τα ενσωματώσει σε αυτά που θα προτείνει κατά το πέρας των διαδικασιών της. Οι χρονικές απαιτήσεις εφαρμογής της EBIOS είναι η βέλτιστη δυνατή καθώς είναι σχεδιασμένη να παρέχει τα πλήρως απαραίτητα αλλά και επαρκή στοιχεία τα οποία απαιτούνται προς επίτευξη του επιθυμητού αποτελέσματος. Το γεγονός αυτό καθιστά την EBIOS μία από τις γρηγορότερες μεθοδολογίες διαχείρισης κινδύνου.

Σε αντίθεση με τα σεναριοστραφή μοντέλα εκτίμησης κινδύνου, η δομημένη προσέγγιση της μεθοδολογίας EBIOS, επιτρέπει την αναγνώριση των στοιχείων κινδύνου όπως οι ευπάθειες, οι μέθοδοι επίθεσης, πράκτορες απειλής και επουσιώδη στοιχεία του πληροφοριακού συστήματος. Αυτή εξονυχιστική και μεθοδική πρακτική, εγγυάται την ολοκληρωτική φύση των αποτελεσμάτων της διαδικασίας ανάλυσης κινδύνου.

Η μεθοδολογία μπορεί να προσαρμοστεί σε οποιοδήποτε διακριτό πλαίσιο και να παραμετροποιηθεί με τον κατάλληλο τρόπο ώστε να μην εκθέσει σε κίνδυνο τις οποιεσδήποτε υπάρχουσες πρακτικές και διαδικασίες και να μην παρεμβαίνει στην φιλοσοφία του οργανισμού. Η ευέλικτη προσέγγιση της EBIOS, προσφέρει πλειάδα εργαλείων στις οντότητες που την εφαρμόζουν, βοηθώντας σε εξαιρετικό βαθμό να διαχειριστούν τον κίνδυνο του οργανισμού. Το εύρος της μπορεί να καλύψει και να εφαρμοστεί από ένα παγκοσμίας διάστασης πληροφοριακό σύστημα, μέχρι ακόμα και μία πολύ μικρού μεγέθους υπηρεσία. Επιλεγμένα μέρη της EBIOS μπορούν να εφαρμοστούν ξεχωριστά, ώστε να παρέχουν υπηρεσίες όπως ανάλυση ευπαθειών ή αναγνώριση στρατηγικών στοιχείων του οργανισμού που χρίζουν αντιμετώπιση υψηλότερης προτεραιότητας από τον οργανισμό όσον αφορά την ασφάλεια τους.

Στηρίζεται σε έννοιες όπως η διακριτή κατηγοριοποίηση οντοτήτων του οργανισμού, οι μέθοδοι επίθεσης, οι ευπάθειες , οι στόχοι ασφαλείας και οι απαιτήσεις ασφαλείας. Οι περισσότερες από αυτές τις έννοιες μπορούν να εφαρμοστούν άμεσα σε ένα ήδη υπάρχον πληροφοριακό σύστημα χωρίς κάποιο ιδιαίτερο πρόβλημα.

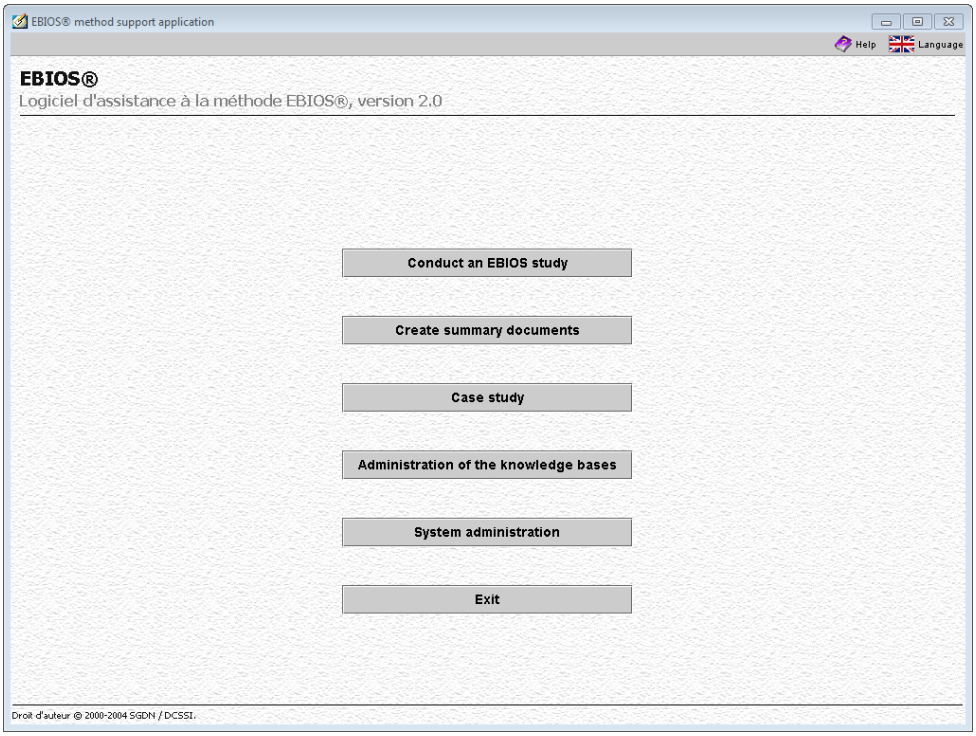
Οι κύριες διαδικασίες στις οποίες βοηθά η μεθοδολογία είναι οι εξής:

- Προετοιμασία κύριου πλάνου πληροφοριακού συστήματος.
- Προετοιμασία πολιτικών ασφαλείας.
- Προετοιμασία πολιτικών πιστοποιήσεων.
- Καταγραφή προφίλ προστασίας.
- Καταγραφή περιγραφών στόχων ασφαλείας.
- Καταγραφή απαιτήσεων ασφαλείας.
- Σύγκριση μεταξύ σχεδίου και πραγματικής εφαρμογής των μέτρων.

3.4.1 EBIOS Case Study

Στα πλαίσια αυτής της πτυχιακής εργασίας, μας παρέχεται το επίσημο λογισμικό της μεθοδολογίας EBIOS, προς εξοικείωση με αυτό. Στην επόμενη ενότητα θα ο αναγνώστης θα περιηγηθεί στο περιβάλλον του λογισμικού και με την συνδρομή του συγγραφέα, θα αποκτήσει μία βαθύτερη και πιο απτή εικόνα της μεθοδολογίας EBIOS.

Με το που ο χρήστης ανοίγει το πρόγραμμα της EBIOS αντικρίζει την εξής εικόνα.

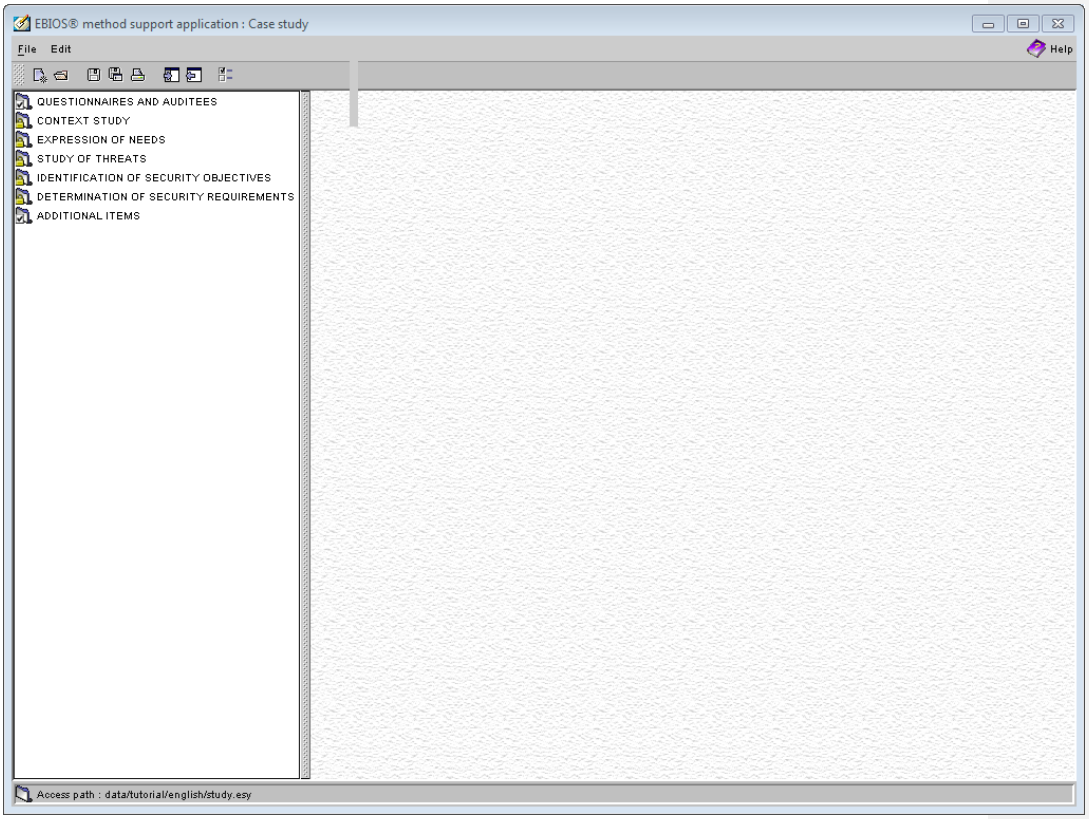


ΕΙΚΟΝΑ 3 ΑΡΧΙΚΟ ΠΑΡΑΘΥΡΟ EBIOS

Το πρόγραμμα παρέχει τις εξής επιλογές:

- Πραγματοποίηση μελέτης κινδύνου βάσει της μεθοδολογίας EBIOS (Conduct an EBIOS study).
- Δημιουργία εγγράφων αναφοράς μελέτης κινδύνου (Create summary documents)
- Παράδειγμα μελέτης κινδύνου (Case study)
- Διαχείριση βάσης δεδομένων (Administration of the knowledge bases)
- Διαχείριση συστήματος (System Administration)
- Έξοδος από το πρόγραμμα (Exit)

Για εκπαιδευτικούς λόγους επιλέγουμε να παρουσιάσουμε πρώτα το παράδειγμα μίας μελέτης κινδύνου, όπως αυτή προσφέρεται έτοιμη από το πρόγραμμα. Επιλέγοντας την αντίστοιχη επιλογή μεταφερόμαστε στο παρακάτω παράθυρο, το οποίο είναι ίδιο με το παράθυρο που θα αντικρίζαμε αν επιλέγαμε να ξεκινήσουμε μία μελέτη από την αρχή.



ΕΙΚΟΝΑ 4 ΠΑΡΑΔΕΙΓΜΑ ΜΕΛΕΤΗΣ EBIOS

Στο αριστερό μέρος της οθόνης μπορούμε να διακρίνουμε τις εξής επιλογές:

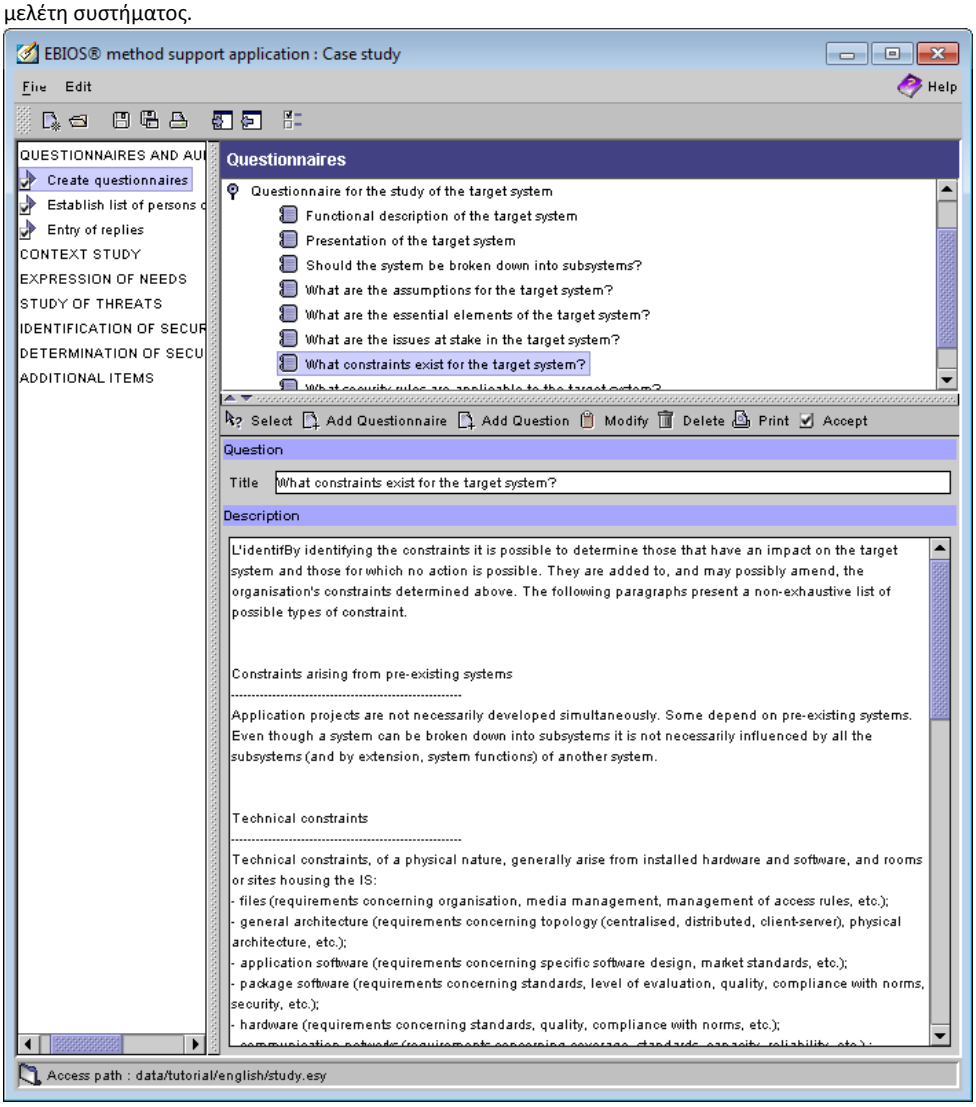
- Questionnaires and Auditees
- Context Study
- Expression of Needs
- Study of Threats
- Identification of Security Objectives
- Determination of Security Requirements
- Additional Items

Κάθε μία από τις παραπάνω επιλογές εξυπηρετεί και έναν διαφορετικό σκοπό της μεθοδολογίας και βοηθούν τον ερευνητή να πραγματοποιήσει την μελέτη όσο το δυνατόν πιο αναίμακτα γίνεται.

3.4.2 Ερωτηματολόγια

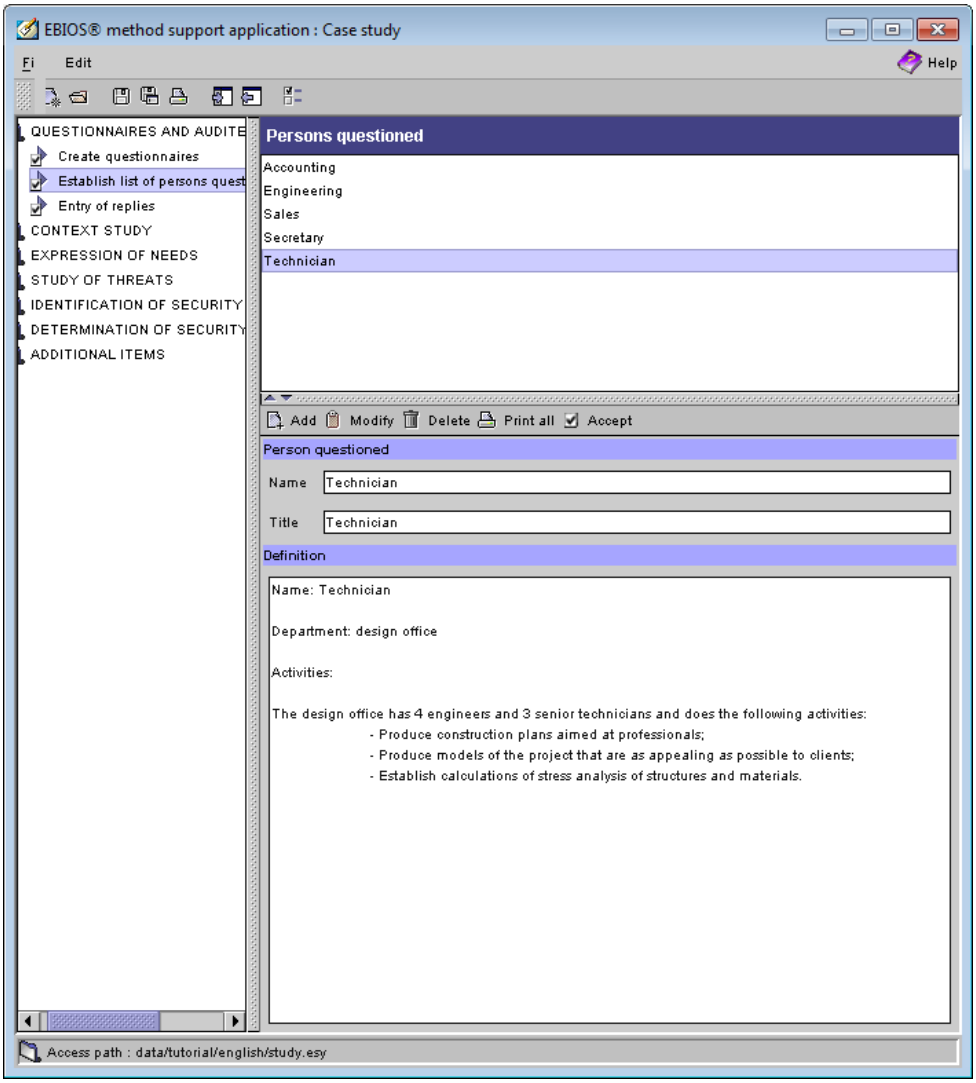
Η πρώτη επιλογή, “Questionnaires and Auditees” αφορά το προκαταρκτικό μέρος της μελέτης ασφαλείας. Κατά την διάρκεια αυτής της φάσης της μελέτης, ο ερευνητής χρησιμοποιεί ερωτηματολόγια για να μάθει περισσότερα για το γενικότερο περιβάλλον του οργανισμού. Το πρόγραμμα υποστηρίζει τον ερευνητή σε αυτή την φάση, δίνοντας του την δυνατότητα να

δημιουργήσει τα κατάλληλα ερωτηματολόγια καθώς επίσης και να καταγράψει τις απαντήσει που έλαβε. Ο ερευνητής μπορεί να δημιουργήσει ερωτηματολόγια και στην συνέχεια να δημιουργήσει ξεχωριστές ερωτήσεις για κάθε ερωτηματολόγιο. Στην παρακάτω εικόνα μπορούμε να δούμε την ερώτηση “What constraints exist for the target system?” στο ερωτηματολόγιο περί ασφάλειας του υπό μελέτη συστήματος.



ΕΙΚΟΝΑ 5 ΕΡΩΤΗΜΑΤΟΛΟΓΙΟ ΕΒΙΟΣ

Στην δεύτερη επιλογή “Establish list of persons questioned” μπορούμε να καταγράψουμε τα άτομα τα οποία ερωτήθηκαν καθώς και λίγα πράγματα για αυτούς.



ΕΙΚΟΝΑ 6 ΛΙΣΤΑ ΕΡΩΤΗΘΕΝΤΩΝ

Τέλος στην επιλογή “Entry of replies” μπορούμε να καταγράψουμε τις απαντήσεις σε όποια ερώτηση επιλέξαμε να πραγματοποιήσουμε.

3.4.3 Μελέτη περιβάλλοντος

Ένα ουσιώδες βήμα της διαδικασίας και πρώτο μέρος της είναι η μελέτη του περιβάλλοντος του οργανισμού. Για να βοηθήσει τον ερευνητή με αυτή την διαδικασία, η EBIOS έχει την επόμενη επιλογή που θα αναλύσουμε, την μελέτη περιβάλλοντος (Context Study). Το πρόγραμμα χωρίζει αυτή την διαδικασία σε τέσσερα επιμέρους βήματα, την μελέτη του οργανισμού, την μελέτη του

συστήματος, την αναγνώριση των στοιχείων ασφαλείας και την επιβεβαίωση του συγκεκριμένου βήματος της διαδικασίας.

Στο πρώτο βήμα καταγράφουμε γενικές πληροφορίες του οργανισμού, όπως τον τομέα στον οποίο δραστηριοποιείται, τις στρατηγικές του, το κεφάλαιο του αλλά και τις πωλήσεις του. Στην συνέχεια καταγράφουμε τους όποιους περιορισμούς μπορεί να αντιμετωπίσουμε από τον οργανισμό. Αυτοί οι περιορισμοί μπορούν να περιλαμβάνουν οποιονδήποτε περιορισμό μπορεί να επηρεάσει τις αποφάσεις που θα πάρει ο ερευνητής σε θέματα ασφαλείας. Οικονομικοί, πολιτικοί και στρατηγικοί περιορισμοί είναι μόνο τρεις από τις κατηγορίες περιορισμών τους οποίους χρειάζεται να έχει στα υπόψη του ο ερευνητής.

Τρίτο σημείο που πρέπει οπωσδήποτε να μελετηθεί από τον ερευνητή είναι ο νομοθετικό και κανονιστικό πλαίσιο υπό το οποίο λειτουργεί ο οργανισμός. Οι εκάστοτε νόμοι και κανόνες, μπορούν να επηρεάσουν το περιβάλλον του οργανισμού και πιο συγκεκριμένα τις εργασιακές συνήθειες των εργαζομένων, την φύση των εργασιών που εκτελεί ο οργανισμός καθώς και τον τρόπο με τον οποίο οφείλουν να ολοκληρωθούν. Επίσης οι συμβατικές υποχρεώσεις ενός οργανισμού εμπίπτουν σε αυτή την κατηγορία και θα πρέπει επίσης να καταγραφούν.

Τέλος, γίνεται καταγραφή του πληροφοριακού συστήματος. Σε αυτό το βήμα της διαδικασίας καταγράφουμε τα πεδία στα οποία εμπλέκεται το πληροφοριακό σύστημα και τα οποία συνεισφέρουν στην επίτευξη των στρατηγικών στόχων του οργανισμού. Σε αυτό το επίπεδο, γίνεται προσπάθεια να αναπαρασταθούν οι τωρινές αλλά και μελλοντικές αλληλεπιδράσεις που υφίστανται μεταξύ των λειτουργικών πεδίων του πληροφοριακού συστήματος και των πεδίων που χρήζουν ασφαλείας. Σκοπός αυτού του βήματος είναι να επισημοποιηθεί η αρχιτεκτονική του συστήματος και να καθοριστούν τα όρια που το χαρακτηρίζουν.

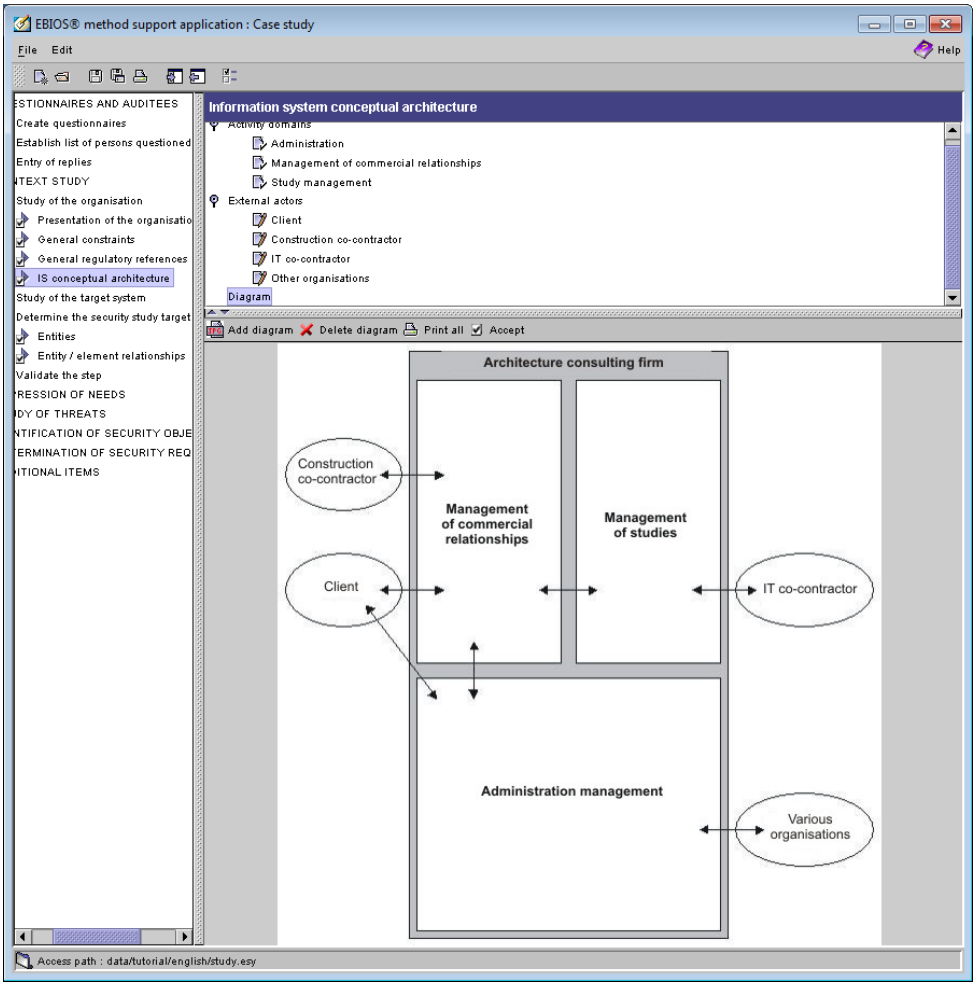
Η EBIOS χωρίζει το πληροφοριακό σύστημα σε δύο μέρη, τα πεδία δραστηριοτήτων και τους εξωτερικούς παράγοντες. Στα πεδία δραστηριοτήτων καθορίζονται τα πεδία στα οποία δραστηριοποιείται το πληροφοριακό σύστημα. Ορισμένα παραδείγματα αποτελούν:

- Η διαχείριση, πχ. Λογιστήριο, νομικό τμήμα, ανθρώπινο δυναμικό.
- Διαχείριση εμπορικών σχέσεων, πχ οι μελέτες και οι εκτιμήσεις τους
- Διαχείριση μελέτης, πχ δημιουργία τεχνικών πλάνων

Στους εξωτερικούς παράγοντες μπορούμε να έχουμε οντότητες όπως:

- Πελάτες
- Κατασκευαστικούς συνεργάτες
- Συνεργάτες πληροφορικής
- Άλλους οργανισμούς

Όλα τα παραπάνω καταγράφονται και στην συνέχεια αποτελούν δομικά στοιχεία στο διάγραμμα που θα αναπαριστά το πληροφοριακό σύστημα και τις αλληλεπιδράσεις μεταξύ των οντοτήτων που το αποτελούν. Παράδειγμα ενός διαγράμματος στην παρακάτω εικόνα.



ΕΙΚΟΝΑ 7 ΔΙΑΓΡΑΜΜΑ ΠΛΗΡΟΦΟΡΙΑΚΟΥ ΣΥΣΤΗΜΑΤΟΣ

Όπως διαπιστώσατε, το παραπάνω διάγραμμα είναι εξαιρετικά αφαιρετικό. Στην προκειμένη φάση της μεθοδολογίας, δεν είναι απαραίτητη η οποιαδήποτε τεχνική εμβάθυνση στο πληροφοριακό σύστημα και συνεπώς παραλείπεται. Στην εικόνα είναι διακριτές οι ξεχωριστές οντότητες του πληροφοριακού συστήματος καθώς και τις αλληλεπιδράσεις μεταξύ οντοτήτων του πληροφοριακού συστήματος και των εξωτερικών παραγόντων.

Εφόσον ως ερευνητές καλύψουμε τις ανάγκες μας για πληροφορία επί του πληροφοριακού συστήματος, προχωρούμε στο επόμενο βήμα. Στο επόμενο βήμα της EBIOS, ο ερευνητής καλείται να μελετήσει το κάθε επί μέρους κομμάτι του πληροφοριακού συστήματος αναλυτικά, εφόσον αυτό πρέπει να συμπεριληφθεί στην μεθοδολογία. Στην επόμενη επιλογή του προγράμματος, μπορούμε να καταγράψουμε πληροφορία όπως:

- Γενική παρουσίαση του συστήματος.
- Προβλήματα.
- Ουσιώδη στοιχεία.
- Λειτουργική περιγραφή.
- Συγκεκριμένοι περιορισμοί.
- Συγκεκριμένες νομικές και κανονιστικές υποχρεώσεις.
- Υποθέσεις.
- Καθορισμός ιεραρχίας χρηστών
- Κανόνες ασφαλείας

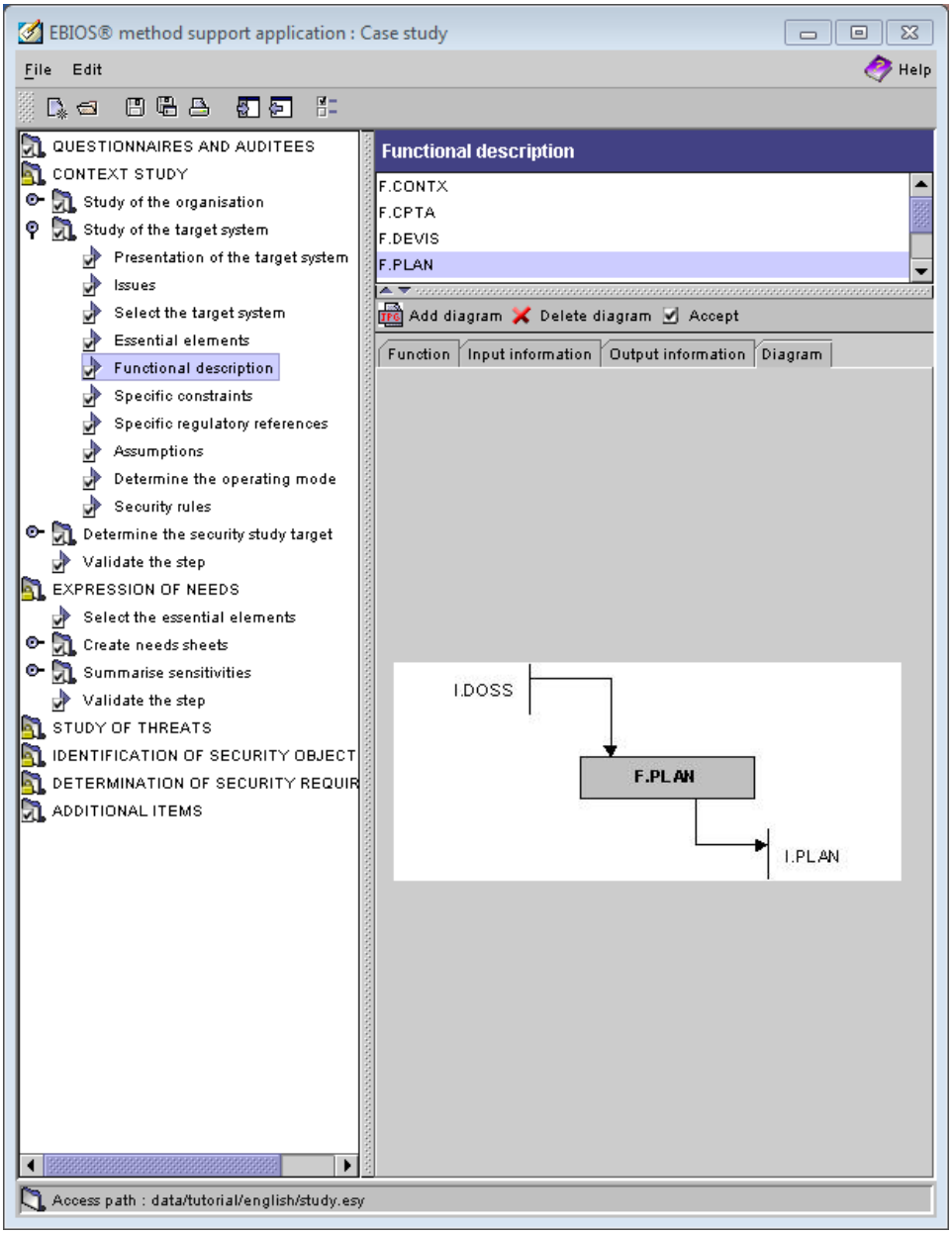
Σκοπός της πρώτης ενότητας πληροφορίας είναι να παρέχει στον ερευνητή μία γενική κάτοψη του συστήματος. Μπορεί να είναι ένα σύστημα ευρείας κλίμακας, ένα υποσύστημα ενός μεγαλύτερου συστήματος ή ακόμα και ένα προϊόν ασφαλείας. Πάραυτα είναι ζωτικής σημασίας να καταγραφεί η συνεισφορά αυτού στο γενικότερο πληροφοριακό σύστημα και τα όρια του.

Στην ενότητα των θεμάτων, ο ερευνητής καταγράφει τα θέματα που του μετέφεραν τα ανώτερα στελέχη του οργανισμού τα οποία θέλουν να αντιμετωπίσουν και αφορούν το σύστημα. Παραδείγματα θεμάτων μπορούν να αποτελούν τα εξής:

- Ανάγκη αύξησης επιπέδων παρεχόμενης υπηρεσίας.
- Αναδιοργάνωση οργανογράμματος
- Ανάγκη αύξησης αποδοτικότητας συναλλαγών με εξωτερικούς συνεργάτες.

Στην συνέχεια έχουμε την επιλογή να καταγράψουμε ουσιώδη στοιχεία του πληροφοριακού συστήματος όπως λειτουργίες του και πληροφορίες τις οποίες μπορεί να επεξεργάζεται ή να χρειάζεται. Αυτές δεν μένουν μόνο στις πληροφορίες οι οποίες είναι σε ψηφιακή μορφή αλλά και αυτές που εισάγονται και από τον φυσικό κόσμο.

Στην ενότητα λειτουργικής περιγραφής, ο αναλυτής αποδίδει μία περιγραφή σε κάθε μία από τις λειτουργίες του πληροφοριακού συστήματος. Κάθε περιγραφή θα πρέπει να περιέχει τις προβλεπόμενες εισόδους και εξόδους τις λειτουργίας, καθώς επίσης και τις διαδικασίες που χρειάζεται να πραγματοποιηθούν για να παραχθούν τα αποτελέσματα τις λειτουργίας. Το πρόγραμμα της EBIOS μας δίνει την δυνατότητα να αναπαραστήσουμε τις διαδικασίες διαγραμματικά.



ΕΙΚΟΝΑ 8 ΔΙΑΓΡΑΜΜΑ ΔΙΑΔΙΚΑΣΙΑΣ

Επόμενο βήμα της EBIOS είναι η καταγραφή συγκεκριμένων περιορισμών που μπορεί να αφορούν το πληροφοριακό σύστημα που εξετάζεται από τον αναλυτή. Αναγνωρίζοντας τους περιορισμούς του πληροφοριακού συστήματος, μπορούμε να καθορίσουμε αυτούς που έχουν σημαντικές επιπτώσεις στο σύστημα. Στην συνέχεια μπορούμε να καταγράψουμε τους νομοθετικούς περιορισμούς. Αναγνωρίζοντας τους νομοθετικούς περιορισμούς στους οποίους υπάγεται το σύστημα, βοηθά τον αναλυτή στο να στοχεύσει καλύτερα στις απαραίτητες συνθήκες οι οποίες είναι απαραίτητες ώστε να λειτουργήσει επαρκώς το πληροφοριακό σύστημα.

Οι υποθέσεις που ενδέχεται να κάνει ο αναλυτής για το πληροφοριακό σύστημα, είναι ανάγκη να καταγραφούν ώστε να επισημοποιηθούν. Οι υποθέσεις συνήθως αφορούν το εσωτερικό ή εξωτερικό περιβάλλον, ακόμα και οικονομικούς ή οργανωτικούς λόγους. Μπορούν επίσης να συνεισφέρουν να καταλάβουμε καλύτερα τους κινδύνους που αποδέχεται ο οργανισμός. Καθώς δημιουργείται ένας στόχος ασφαλείας ο οποίος είναι ανάγκη να επιδείξει ότι καλύπτει την ανάγκη ασφαλείας στην οποία στοχεύει, αναπόφευκτα ενδέχεται να υπάρχουν ευπάθειες οι οποίες δεν καλύπτονται από κάποιο στόχο ασφάλειας. Υπό αυτή την οπτική γωνία θα πρέπει να υπάρχει μία επίσημη αναγνώριση ότι υπάρχει γνώση συγκεκριμένων περιορισμών.

Στην συνέχεια ο αναλυτής καλείται να καθορίσει τα επίπεδα χρηστών τα οποία εξυπηρετεί το σύστημα. Η πιο συνηθισμένη πρακτική είναι να αποδίδονται αριθμητικές τιμές σε αντίστοιχες ομάδες δικαιωμάτων. Έτσι δημιουργούνται ξεκάθαρες βαθμίδες χρηστών οι οποίες είναι εύκολα διακριτές. Αυτή η πρακτική επιτρέπει στην ευκολότερη κατανόηση των προβλημάτων ασφαλείας. Το σχήμα που θα κατασκευαστεί δεν είναι ανάγκη να είναι στατικό. Μπορούμε να αναθεωρήσουμε το συγκεκριμένο σχήμα αφότου πραγματοποιηθεί η διαδικασία διαχείρισης κινδύνου.

Σε αυτό το σημείο πιθανώς έχει δημιουργηθεί μία βασική γραμμή της μελέτης καθώς επίσης και να έχουν συνταχθεί ορισμένα από τα έγγραφα περί της ασφάλειας του πληροφοριακού συστήματος. Αν και μία πλήρως αναλυτική ανάλυση δεν θα ήταν πλήρως εκμεταλλεύσιμη. Ωστόσο μπορούμε να εξάγουμε πληροφορία όπως προτεραιότητες και πρώιμα αποτελέσματα. Στόχος της ενότητας των κανόνων ασφαλείας είναι να αναγνωριστούν οι κύριοι κανόνες και μέτρα ασφαλείας τα οποία θα εφαρμοστούν στο τέλος της διαδικασίας. Τα δεδομένα που εξάγονται από αυτό το βήμα, μπορούν να χρησιμοποιηθούν σε:

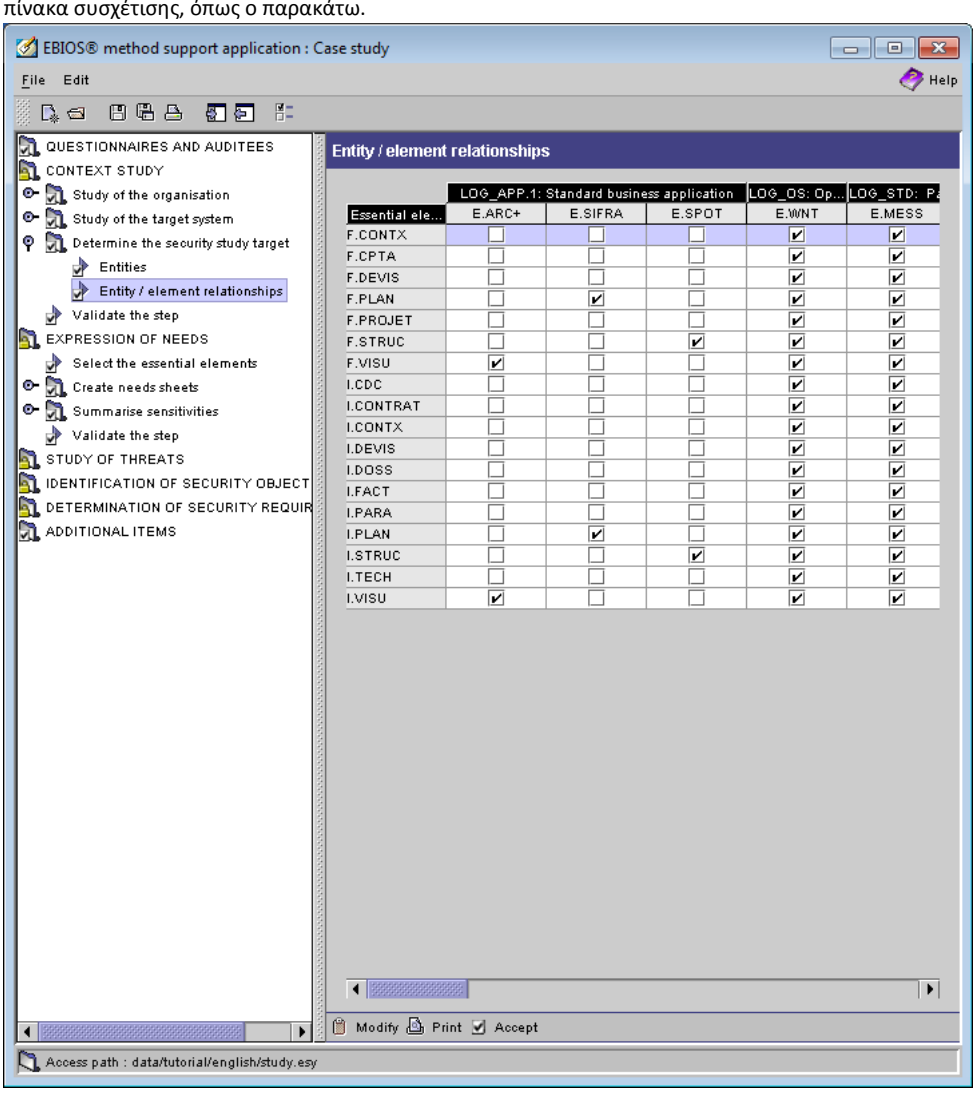
- Σύνταξη πολιτικής ασφαλείας
- Σχέδιο επιχειρηματικής συνέχειας
- Οδηγίες ασφαλείας
- Επιθεωρήσεις ασφαλείας

Τελευταίο βήμα στην μελέτη περιβάλλοντος είναι να καθορίσουμε τα στοιχεία πάνω στα οποία στηρίζεται η προστασία του πληροφοριακού συστήματος. Με αυτόν τον τρόπο είναι δυνατόν να δημιουργηθούν πίνακες συσχετίσεων μεταξύ οντοτήτων και διαδικασιών του συστήματος. Αρχικά ο αναλυτής καταγράφει όλα τα στοιχεία τα οποία χρειάζονται για να πραγματοποιηθεί αυτό το βήμα. Σε αυτά μπορεί να συμπεριληφθούν στοιχεία όπως:

- Λογισμικό
- Υλισμικό
- Μεταφερόμενος εξοπλισμός

Στην συνέχεια δημιουργούμε τον πίνακα συσχετίσεων. Στον άξονα Υ έχουμε τις διάφορες διαδικασίες του πληροφοριακού συστήματος οι οποίες έχουν καταγραφεί σε προηγούμενο βήμα. Στον Χ άξονα

καταγράφονται οι οντότητες του πληροφοριακού συστήματος. Έτσι μπορούμε να δημιουργήσουμε πίνακα συσχέτισης, όπως ο παρακάτω.



ΕΙΚΟΝΑ 9 ΠΙΝΑΚΑΣ ΣΥΣΧΕΤΙΣΗΣ ΟΝΤΟΤΗΤΩΝ – ΔΙΑΔΙΚΑΣΙΩΝ

Τελευταίο βήμα στην μελέτη του περιβάλλοντος του οργανισμού είναι να επικυρωθούν τα καταγεγραμμένα δεδομένα από κάποια επικυρωτική αρχή. Συνήθως αυτή αποτελείται από το διοικητικό συμβούλιο και τα ανώτερα στελέχη των τμημάτων του οργανισμού. Επικυρώνοντας τα δεδομένα, ο αναλυτής μπορεί να είναι σίγουρος πως όλα τα εμπλεκόμενα μέλη βρίσκονται στο ίδιο μήκος κύματος και δεν υπάρχουν ασυνέχειες στα δεδομένα.

3.4.4 Έκφραση αναγκών

Επόμενο βήμα της μεθοδολογίας EBIOS είναι η έκφραση αναγκών. Έχοντας αναγνωρίσει και μελετήσει το σύστημα μέσω του προηγούμενου βήματος, σειρά έχει η περιγραφή των αναγκών του κάθε κρίσιμου στοιχείου που αποτελεί το σύστημα. Οι ανάγκες ασφαλείας που σχετίζονται με ένα πληροφοριακό σύστημα και τις διεργασίες του, εκφράζονται κυρίως μέσω των ακόλουθων κριτηρίων:

- Διαθεσιμότητα
- Ακεραιότητα
- Εμπιστευτικότητα

Αυτά τα κριτήρια δεν είναι τα μοναδικά τα οποία μπορούμε να χρησιμοποιήσουμε. Οι ανάγκες ασφαλείας μπορούν να εκφραστούν και με επιπρόσθετους όρους όπως η επίβλεψη (Monitoring – Audit) και η ανωνυμία. Μπορεί να είναι οποιοσδήποτε όρος ο οποίος αναφέρεται στην βάση γνώσης της εκάστοτε μελέτης ο οποίος μπορεί να εκθέσει το πληροφοριακό σύστημα. Η βάση γνώσης της εκπαιδευτικής μελέτης περιέχει μόνο τους τρεις πρώτους προαναφερθέντες όρους.

Στην συνέχεια υπάρχει η ανάγκη να δημιουργήσουμε μία μετρική η οποία θα μας βοηθά να περιγράψουμε τις ανάγκες ασφαλείας ενός στοιχείου. Για κάθε διακριτή τιμή της μετρικής και κάθε κριτήριο μπορούμε να ορίσουμε τις απαιτήσεις ασφαλείας που χρειαζόμαστε. Έστω ότι έχουμε τρία επίπεδα ασφαλείας, τα οποία ονομάζουμε 1,2,3. Αυτό το επίπεδο λειτουργεί ως ταμπέλα για το στοιχείο του πληροφοριακού συστήματος. Κάθε επίπεδο ασφαλείας μπορεί να έχει διαφορετικές επίπεδα αναγκών για κάθε ορισμένο κριτήριο. Για παράδειγμα το κριτήριο ασφαλείας διαθεσιμότητας, στο επίπεδο ασφαλείας 1 μπορεί να ορίζει πως το στοιχείο ασφαλείας μπορεί να παραμείνει μη διαθέσιμο για κάποιο ορισμένο χρονικό διάστημα, χωρίς συνέπειες. Το ίδιο κριτήριο ασφαλείας, σε υψηλότερο επίπεδο ασφαλείας, μπορεί να ορίζει πως το μέγιστο χρονικό διάστημα μη διαθεσιμότητας ενός στοιχείου είναι μερικά δευτερόλεπτα. Τα επίπεδα και οι ανάγκες ασφαλείας καθορίζονται βάσει των πληροφοριών που έχει αποκομίσει ο αναλυτής από το προηγούμενο βήμα, αυτό της μελέτης του περιβάλλοντος. Εμμέσως, ο οργανισμός είναι αυτός που καθορίζει τις ανάγκες.

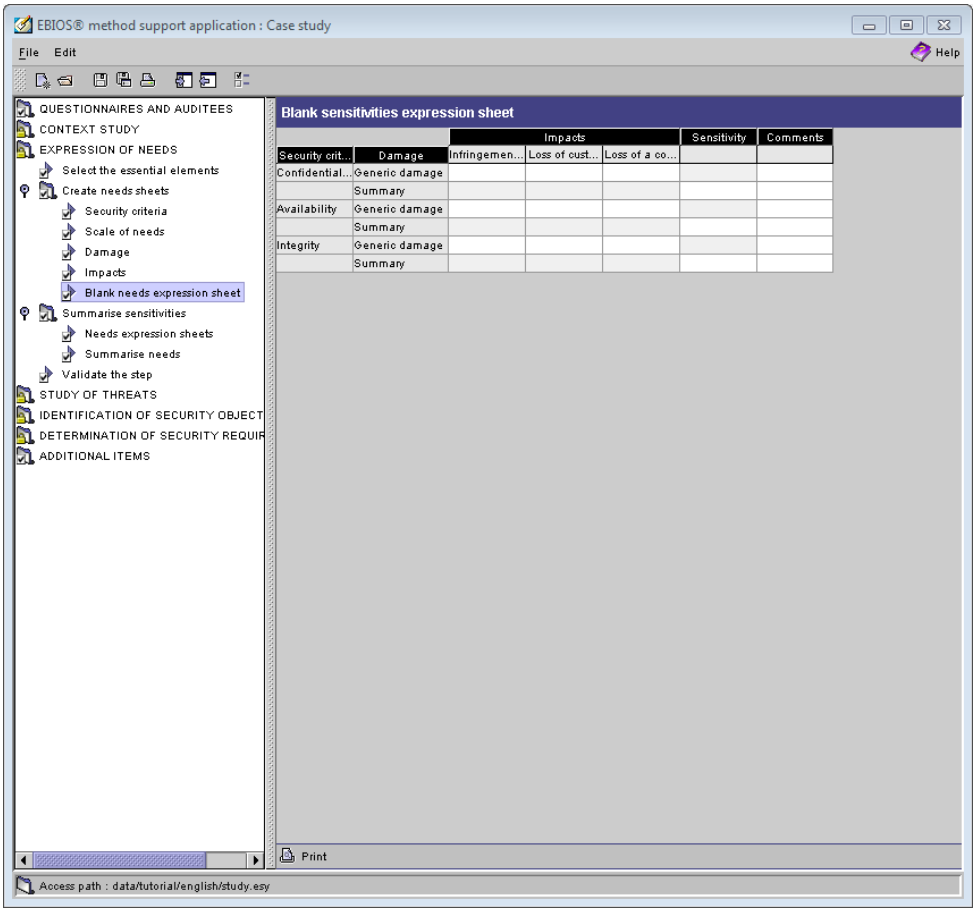
Στην συνέχεια για κάθε κριτήριο ασφαλείας καλούμαστε να περιγράψουμε ένα συμβάν που τα εκθέτει. Αυτό γίνεται για να γίνει ευκολότερο το επόμενο βήμα, αυτό της μελέτης επιπτώσεων της έκθεσης κάποιου κριτηρίου ασφαλείας. Προς αποσαφήνιση των όρων ζημία και επίπτωση, αναλογιστείτε το εξής περιστατικό. Έστω ότι κάποιος κόβει το χέρι του με ένα μαχαίρι. Αναλόγως της έκτασης της ζημίας που έχει προκληθεί μπορούμε να έχουμε τις εξής επιπτώσεις:

- Μικρή ενόχληση του ατόμου στην καθημερινότητά του.
- Μείωση επιπέδου επιδεξιότητας του συγκεκριμένου άκρου.
- Θάνατος.

Λόγω του ότι τα συμβάντα που μπορούν να προκαλέσουν ζημιά είναι πάρα πολλά, συνηθίζεται να αναγράφουμε ένα μοναδικό περιστατικό ως γενικής φύσεως περιστατικό και στην συνέχεια να καταγράφουμε τις διάφορες γενικές επιπτώσεις που μπορεί να κληθεί να αντιμετωπίσει ο οργανισμός. Στο σύμπαν του πληροφοριακού συστήματος ορισμένα παραδείγματα επιπτώσεων είναι:

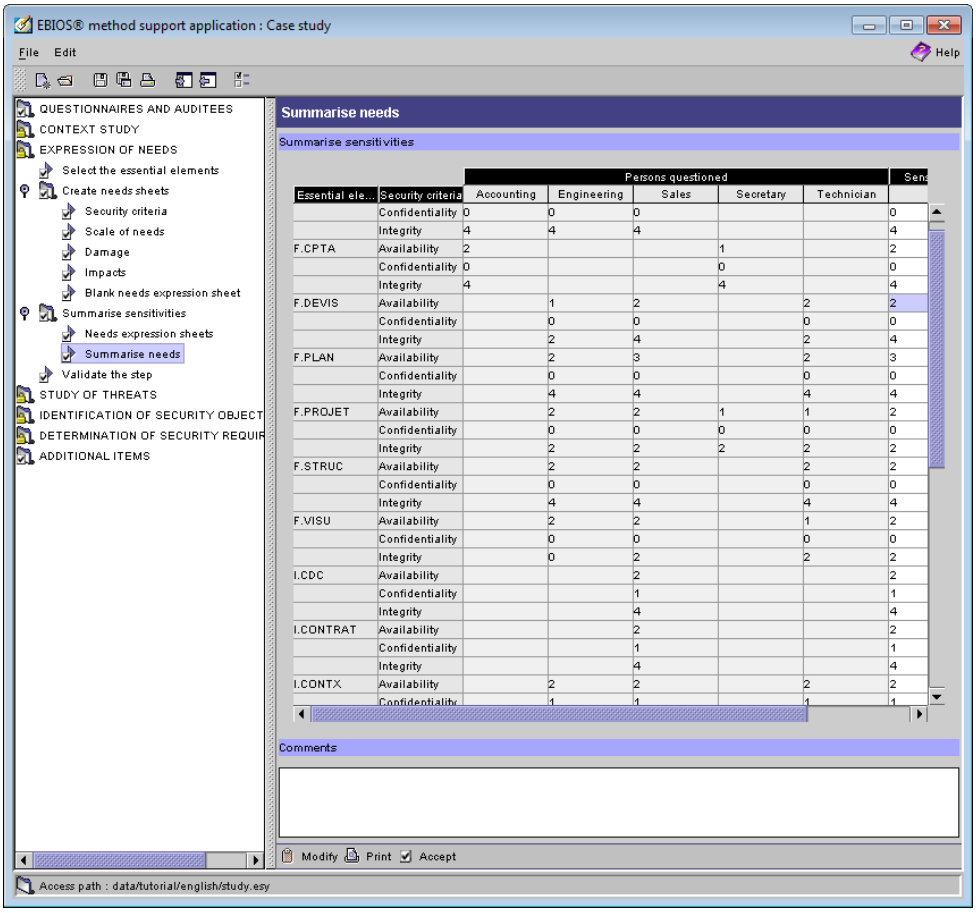
- Παραβίαση νόμων ή/και κανονισμών.
- Απώλεια ανταγωνιστικότητας.
- Απώλεια εμπιστοσύνης αγοραστικού κοινού.

Έχοντας συμπληρώσει τις άνωθεν πληροφορίες, μπορούμε να δημιουργήσουμε τα φυλλάδια αναγκών ασφαλείας. Το φυλλάδιο, αποτελείται από έναν πίνακα ο οποίος συνίσταται από όλα τα στοιχεία τα οποία έχουμε συλλέξει προηγουμένως.



ΕΙΚΟΝΑ 10 ΦΥΛΛΑΔΙΟ ΑΝΑΓΚΩΝ ΑΣΦΑΛΕΙΑΣ

Αυτά τα φυλλάδια εκτυπώνονται και διαμοιράζονται στα κατάλληλα άτομα προς συμπλήρωσή τους. Θα πρέπει να αντιστοιχεί ένα φυλλάδιο για κάθε λειτουργία και κάθε στοιχείο του πληροφοριακού συστήματος. Αφότου συμπληρωθούν τα φυλλάδια, τα δεδομένα συγκεντρώνονται σε ένα κεντρικό πίνακα ο οποίος περιέχει όλα τα στοιχεία τα οποία συλλέχθηκαν. Σε αυτόν τον πίνακα θα αναγράφεται το επίπεδο ασφαλείας της εκάστοτε διαδικασίας ή στοιχείου. Στην περίπτωση που κάποιο στοιχείο ή διαδικασία έχει βαθμονομηθεί διαφορετικά από τους ερωτηθέντες, ως ταμπέλα ασφαλείας ορίζεται αυτή που έχει επιλεχθεί από περισσότερα άτομα.



ΕΙΚΟΝΑ 11 ΠΙΝΑΚΑΣ ΕΠΙΠΕΔΩΝ ΑΣΦΑΛΕΙΑΣ

Εφόσον δημιουργηθεί ο συγκεκριμένος πίνακας, επόμενη κίνηση του αναλυτή είναι να συναντηθεί με τα αρμόδια άτομα στον οργανισμό τα οποία θα επιβεβαιώσουν τα δεδομένα που έχουν συλλεχθεί, το οποίο θα σημάνει πράσινο φως για τον αναλυτή να προχωρήσει στο επόμενο βήμα της μεθοδολογίας EBIOS, αυτό της μελέτης απειλών.

3.4.5 Μελέτη απειλών

Σε αυτό το στάδιο, ο αναλυτής πραγματοποιεί μελέτη των απειλών που μπορούν να εκθέσουν το πληροφοριακό σύστημα και τις διαδικασίες του. Η μελέτη περιλαμβάνει περιγραφή των μεθόδων επίθεσης και των στοιχείων που επιβαρύνονται από μία ενδεχόμενη επίθεση, καθώς και τις συ σχετιζόμενες εκμεταλλεύσιμες αδυναμίες. Με το πέρας αυτής της διαδικασίας, ο αναλυτής θα είναι σε θέση να περιγράψει τις διάφορες απειλές που μπορούν να εκθέσουν το πληροφοριακό σύστημα ώστε να καταστεί δυνατή η αντιμετώπισή τους με τον πλέον κατάλληλο τρόπο.

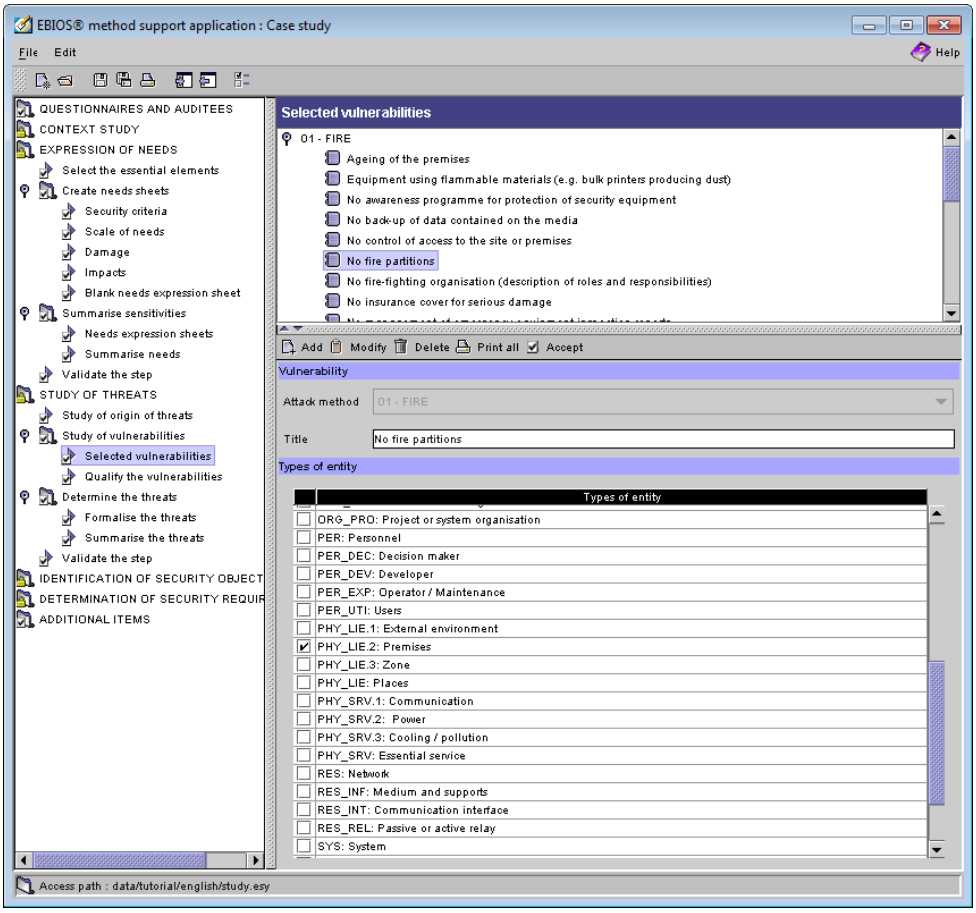
Στην βάση γνώσης της εφαρμογής καταγράφεται μία πλειάδα απειλών οι οποίες μπορούν να επηρεάσουν το πληροφοριακό σύστημα. Σε αυτό το βήμα, ο αναλυτής διαλέγει ποιες από αυτές τις απειλές θεωρεί ο οργανισμός πως μπορούν να επηρεάσουν το πληροφοριακό σύστημα και είναι σε θέση να τις αντιμετωπίσουν. Για κάθε απειλή είναι καταγεγραμμένη πληροφορία όπως:

- Τύπος (Φυσικός φαινόμενο, Ανθρώπινος παράγοντας, Περιβαλλοντικός παράγοντας κ.α.)
- Πρόκληση εξ ατυχήματος (Συγκέντρωση εύφλεκτων υλικών σε περιβάλλον που ευνοεί την πρόκληση φωτιάς).
- Ηθελημένη πρόκληση (Τρομοκρατική επίθεση).
- Τύποι επιπτώσεων (Καταστροφή στοιχείων, οικονομική ζημιά).

Για κάθε απειλή, πρέπει επίσης να καταγράψουμε ποιο κριτήριο ασφαλείας εκτίθεται σε περίπτωση εμφάνισης της απειλής.

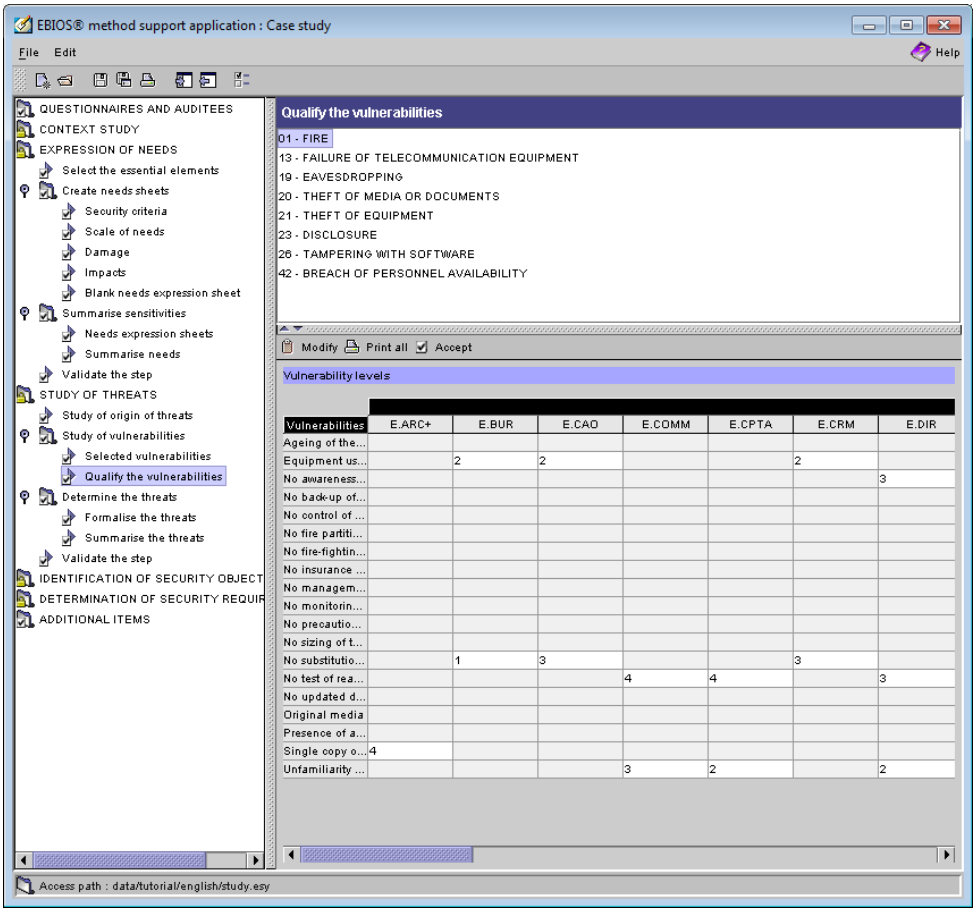
Ακόλουθο βήμα του αναλυτή είναι η μελέτη των ευπαθειών που θα επιτρέψουν στην απειλή να επιφέρει συνέπειες στον οργανισμό. Για κάθε απειλή που έχει καταγραφεί στο προηγούμενο μέρος, καθορίζουμε τις σχετικές ευπάθειες και τις βαθμολογούμε βάσει της πιθανότητας να συμβεί, ή με την συχνότητα με την οποία εμφανίζεται. Οι παράγοντες που θα καθορίσουν την βαθμολογία που θα αποδοθεί στην κάθε απειλή, καθορίζονται κατά την μελέτη του περιβάλλοντος του οργανισμού.

Για κάθε απειλή διαλέγουμε τις ευπάθειες που μπορούν να την καταστήσουν δυνατή και καθορίζουμε ποια στοιχεία του πληροφοριακού συστήματος θα επηρεαστούν σε περίπτωση εμφάνισής της. Κάθε ευπάθεια μπορεί να επηρεάζει διαφορετικά στοιχεία, αλλά η απειλή να παραμένει ίδια. Για αυτό τον λόγο καταγράφουμε τα επηρεαζόμενα στοιχεία για κάθε ευπάθεια ξεχωριστά.



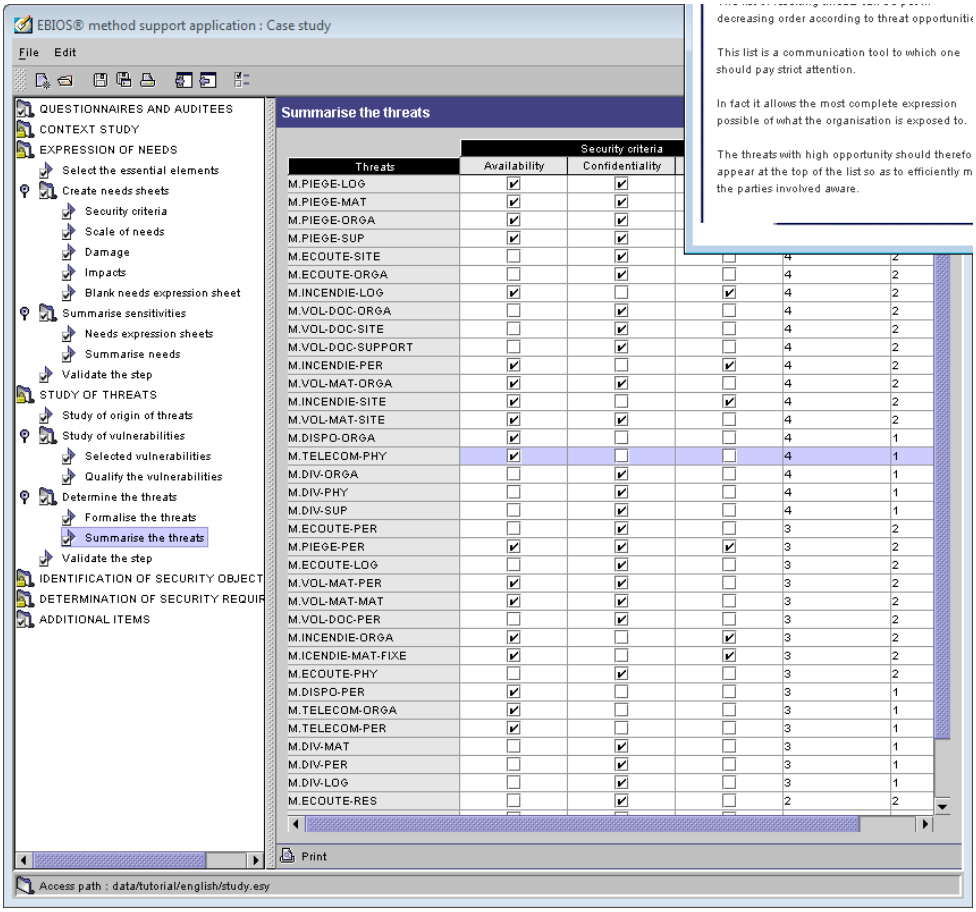
ΕΙΚΟΝΑ 12 ΣΥΣΧΕΤΙΣΗ ΕΥΠΑΘΕΙΑΣ ΑΠΕΙΛΗΣ ΚΑΙ ΕΠΗΡΕΑΖΟΜΕΝΟΥ ΣΤΟΙΧΕΙΟΥ

Στην συνέχεια βαθμολογούμε κατά πόσο επηρεάζουν οι ευπάθειες κάθε απειλής, τα στοιχεία του πληροφοριακού συστήματος.



ΕΙΚΟΝΑ 13 ΒΑΘΜΟΛΟΓΙΑ ΕΥΠΑΘΕΙΩΝ

Στο επόμενο βήμα, η μεθοδολογία μας βοηθά να ταξινομήσουμε τις απειλές και να μας βοηθήσει να τις κατανοήσουμε καλύτερα, προσφέροντας μας τα εργαλεία να δημιουργήσουμε έναν πίνακα ο οποίος θα περιέχει όλη την πληροφορία συγκεντρωμένη. Σε αυτόν τον πίνακα θα αναγράφεται η απειλή, αν επηρεάζει κάποιο κριτήριο ασφαλείας, πόσο θα επηρεάσει τον οργανισμό και πόσο πιθανή είναι να πραγματοποιηθεί.



ΕΙΚΟΝΑ 14 ΠΙΝΑΚΑΣ ΜΕΛΕΤΗΣ ΑΠΕΙΛΩΝ

Ο συγκεκριμένος πίνακας αποτελεί ένα πολύ χρήσιμο εργαλείο στην προσπάθεια του αναλυτή να επικοινωνήσει τον κίνδυνο προς τα άτομα τα οποία τα αφορά η διαδικασία διαχείρισης κινδύνου που πραγματοποιείται. Τελευταίο και συνηθισμένο πλέον βήμα για την φάση της μελέτης απειλών είναι η επιβεβαίωση των δεδομένων που έχουν συλλεχθεί και της πληροφορίας που έχει παραχθεί από τα αρμόδια άτομα.

3.4.6 Αναγνώριση σκοπών ασφαλείας

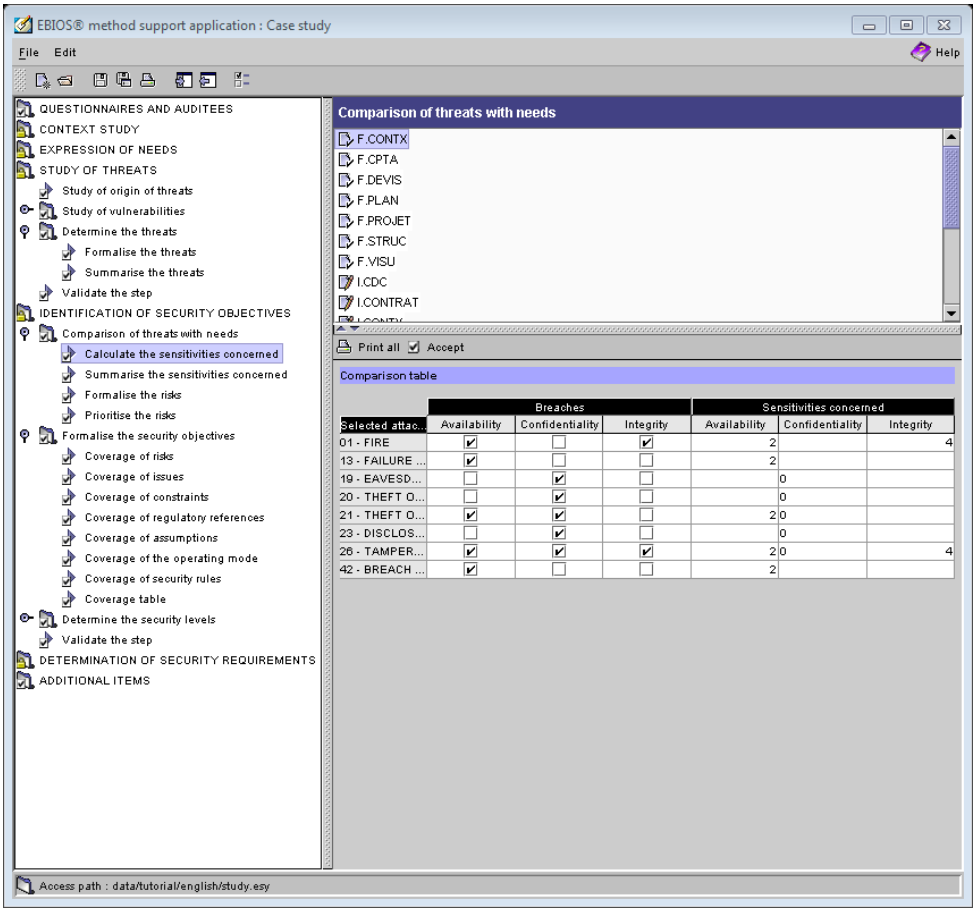
Στα προηγούμενα βήματα, επισημοποιήσαμε το πως εκφράζονται τα επίπεδα ασφαλείας των στοιχείων του πληροφοριακού συστήματος και των συ σχετιζόμενων διαδικασιών του οργανισμού. Επίσης αναγνωρίσαμε τις απειλές που μπορεί να εκθέσουν τον οργανισμό σε κίνδυνο. Σε αυτό το στάδιο της μεθοδολογίας EBIOS, θα προσπαθήσουμε να προσδιορίσουμε την πιθανότητα μία συγκεκριμένη απειλή όντως να επηρεάσει τον οργανισμό. Όλοι οι κίνδυνοι, οι υποθέσεις και οι κανόνες

ασφαλείας θα πρέπει να καλύπτονται πλήρως από τους σκοπούς ασφαλείας, έχοντας υπόψη τυχόν περιορισμούς από το περιβάλλον του οργανισμού.

Η πρώτη δραστηριότητα του συγκεκριμένου σταδίου στην μεθοδολογία είναι να προσδιορίσουμε, επισημοποιήσουμε και να θέσουμε προτεραιότητες στους πραγματικούς κινδύνους του πληροφοριακού συστήματος. Αυτό πραγματοποιείται μέσω μίας διαδικασίας σύγκρισης των απειλών με τις ανάγκες του συστήματος.

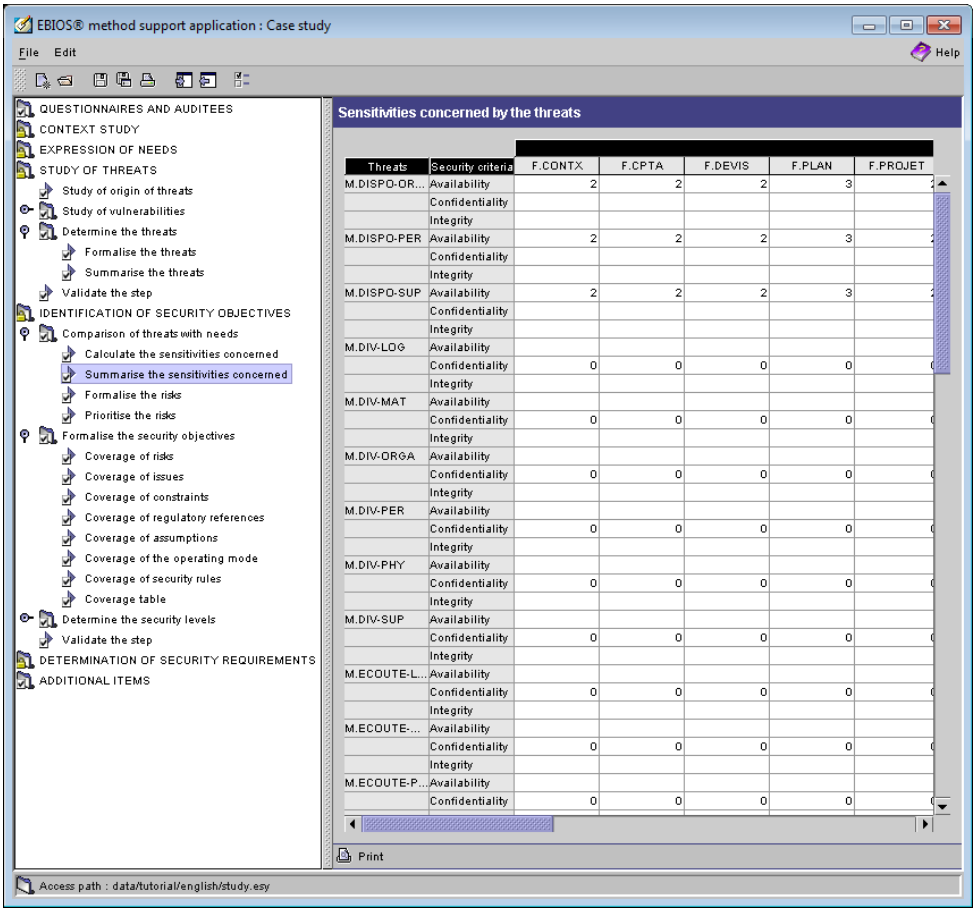
Με την βοήθεια των προσδιορισμένων αναγκών ασφαλείας για κάθε ουσιώδες στοιχείο του πληροφοριακού συστήματος, για τα οποία έχουμε πλέον αριθμητικές τιμές βάσει της ταμπέλας ασφαλείας που του έχουμε προδιαγράψει και τις απειλές που προσδιορίσαμε στο προηγούμενο βήμα, μπορούμε να προσδιορίσουμε αν κάποια αναγραφόμενη απειλή μπορεί πραγματικά να επηρεάσει το πληροφοριακό σύστημα.

Η σύγκριση των αναγκών με τις απειλές γίνεται βάσει ενός πίνακα που αναγράφει την κατάλληλη πληροφορία. Για κάθε στοιχείο του πληροφοριακού συστήματος και κάθε διαδικασία, η μεθοδολογία EBIOS δημιουργεί έναν πίνακα στον οποίο τοποθετεί τις ανάγκες δίπλα στις απειλές.



ΕΙΚΟΝΑ 15 ΣΥΓΚΡΙΣΗ ΑΝΑΓΚΩΝ – ΑΠΕΙΛΩΝ

Συμπληρωματικά, η μεθοδολογία προσφέρει και έναν επιπλέον συγκεντρωτικό πίνακα, πιθανώς για λόγους επικοινωνίας των απειλών και των αναγκών.

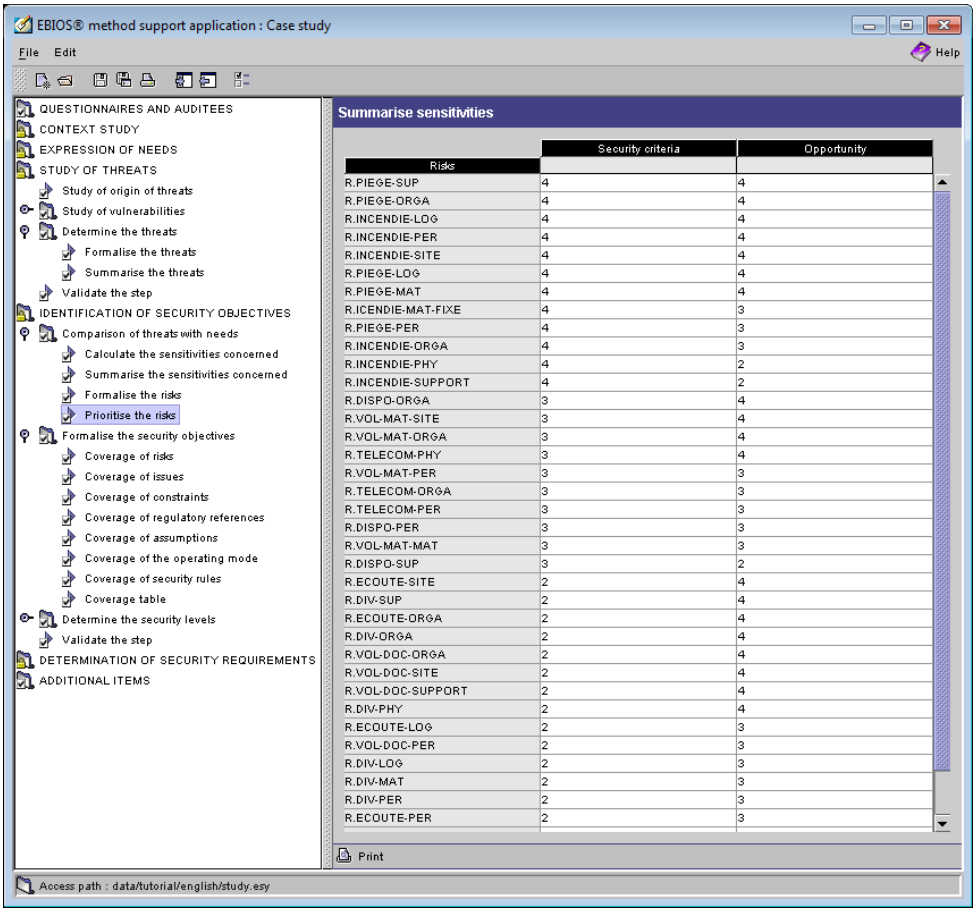


ΕΙΚΟΝΑ 16 ΕΠΙΚΟΙΝΩΝΙΑΚΟΣ ΠΙΝΑΚΑΣ ΑΝΑΓΚΩΝ – ΑΠΕΙΛΩΝ

Χρησιμοποιώντας τον προηγούμενο πίνακα, δηλαδή τις απειλές και τις ανάγκες ασφαλείας, μπορούμε να δημιουργήσουμε ενδείξεις κινδύνου οι οποίες μπορούν να είναι όσο αναλυτικές χρειάζεται. Μία ένδειξη κινδύνου μπορεί να περιέχει πληροφορία όπως:

- Την απειλή και τα χαρακτηριστικά της, κυρίως την πιθανότητα εμφάνισής της.
- Την μέθοδο εμφάνισης.
- Τις ευπάθειες που σχετίζονται μαζί της.
- Τις οντότητες που φέρουν τις εν λόγω ευπάθειες.
- Τις επιπτώσεις που αποφέρουν στον οργανισμό, βάσει των αναγκών ασφαλείας

Στην συνέχεια θέτουμε προτεραιότητα στους κινδύνους, βάσει των στοιχείων που μόλις συλλέξαμε και συγκεντρώνουμε όλη την πληροφορία σε έναν πίνακα.



ΕΙΚΟΝΑ 17 ΠΡΟΤΕΡΑΙΟΤΗΤΑ ΚΙΝΔΥΝΩΝ

Οι σκοποί ασφαλείας οφείλουν να καλύπτουν όλους τους κινδύνους και να λαμβάνουν υπόψη τους διάφορα στοιχεία του οργανισμού τα οποία μπορούν να επηρεάζουν την όλη διαδικασία, όπως οι κανόνες ασφαλείας για παράδειγμα. Το ποσοστό εκπλήρωσης της κάλυψης των κινδύνων, πρέπει να επιδεικνύεται βάσει:

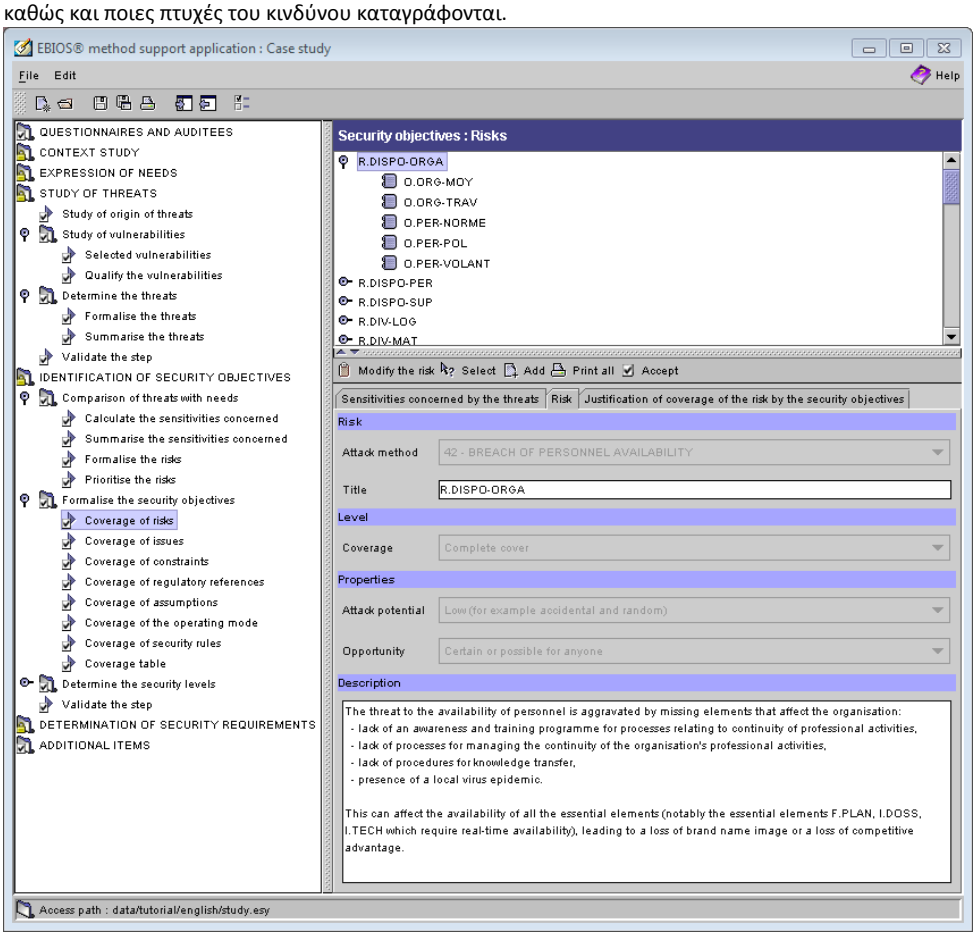
- Του τρόπου με τον οποίο οι σκοποί ασφαλείας καλύπτουν όλους τους κινδύνους, τους κανόνες ασφαλείας που έχουν τεθεί αλλά και τις όποιες κανονιστικές διατάξεις στις οποίες υπόκειται ο οργανισμός
- Επιδεικνύοντας ότι οι σκοποί ασφαλείας είναι σχετικοί με το γενικότερο περιβάλλον της εφαρμογής τους και συνεπώς με τους κινδύνους τους οποίους μπορεί να έχουν κληθεί να καλύψουν.

Αρχικά, καλύπτουμε όλους τους κινδύνους οι οποίοι έχουν αναγνωριστεί από τους σκοπούς ασφαλείας και επιδεικνύουμε την πλήρη κάλυψή τους. Ένας κίνδυνος μπορεί να καλύπτεται από πολλούς σκοπούς

ασφαλείας όπως επίσης ένας σκοπός ασφαλείας μπορεί να καλύπτει πολλαπλούς κινδύνους. Στοιχεία των καλυπτόμενων από τους σκοπούς ασφαλείας κινδύνων, αποτελούν:

- Η πηγή της απειλής.
- Οι ευπάθειες.
- Οι συνέπειες.

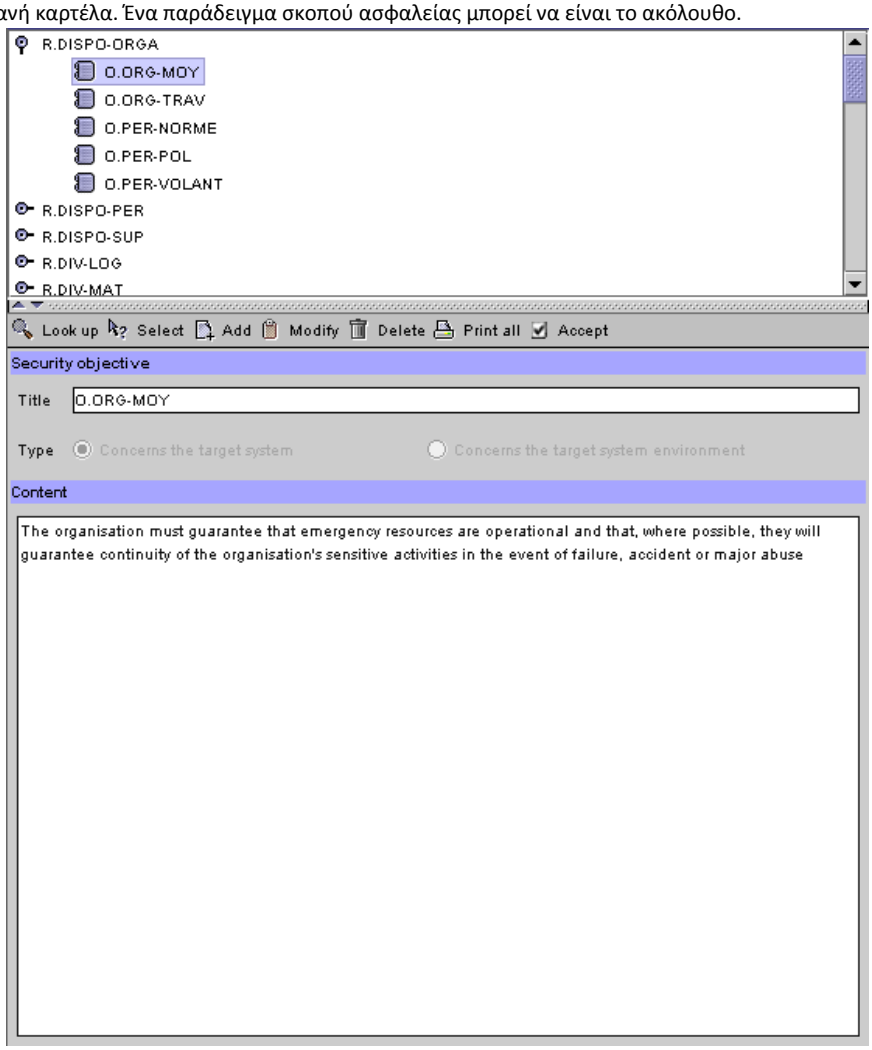
Η μεθοδολογία EBIOS βοηθά τον αναλυτή να καταγράψει κατάλληλα την ζητούμενη πληροφορία δίνοντάς του τα κατάλληλα εργαλεία. Για κάθε αναγνωρισμένο κίνδυνο καταγράφονται οι σκοποί ασφαλείας που αφορούν τον συγκεκριμένο κίνδυνο. Επίσης καταγράφεται μία περιγραφή του κινδύνου,
καθώς και ποιες πτυχές του κινδύνου καταγράφονται.



ΕΙΚΟΝΑ 18 ΠΕΡΙΓΡΑΦΗ ΣΤΟΙΧΕΙΩΝ ΚΙΝΔΥΝΟΥ

Στην παραπάνω εικόνα μπορούμε να δούμε πως η EBIOS έχει καταχωρήσει τους σκοπούς ασφαλείας οι οποίοι είναι σχετικοί για κάθε κίνδυνο. Κάθε κίνδυνος έχει τους δικούς του σκοπούς ασφαλείας οι

οποίοι μπορούν να εμφανίζονται και σε άλλους κινδύνους. Προσφέρεται η επιλογή στον αναλυτή να περιγράψει τον κίνδυνο καθώς και να καταγράψει ποιες ευπάθειες στοχεύουν οι σκοποί ασφαλείας σε διπλανή καρτέλα. Ένα παράδειγμα σκοπού ασφαλείας μπορεί να είναι το ακόλουθο.



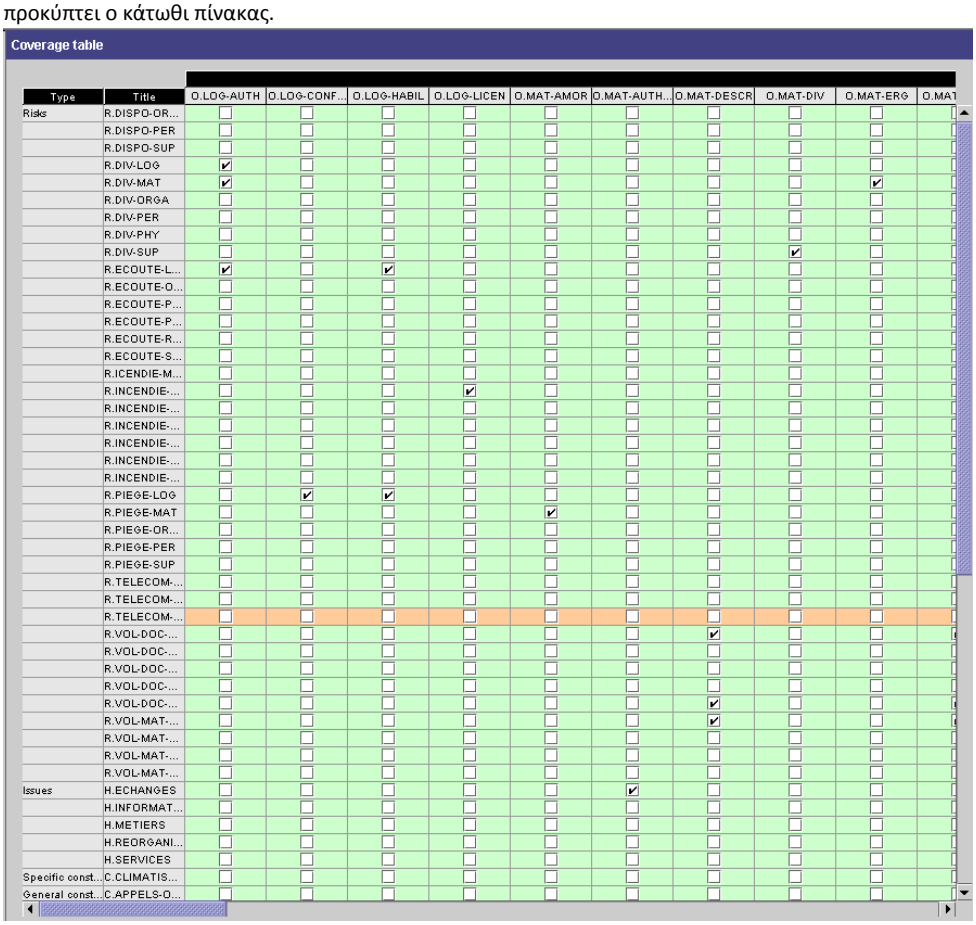
ΕΙΚΟΝΑ 19 ΣΚΟΠΟΣ ΑΣΦΑΛΕΙΑΣ

Επίσης, τα:

- Ζητήματα
- Περιορισμοί
- Κανονιστικές διατάξεις
- Υποθέσεις
- Λειτουργικό πλαίσιο

- Κανόνες ασφαλείας

καταγράφονται με παρόμοιο τρόπο. Τέλος, εφόσον έχει καταγραφεί όλη αυτή η πληροφορία προκύπτει ο κάτωθι πίνακας.



ΕΙΚΟΝΑ 20 ΠΙΝΑΚΑΣ ΚΑΛΥΨΗΣ

Στο παραπάνω πίνακα μπορούμε να δούμε πως σχετίζονται οι διάφοροι σκοποί ασφαλείας με τους κίνδυνους, τα ζητήματα και όσα άλλα αναφέραμε προηγουμένως. Καθ' αυτό τον τρόπο γίνεται εύκολη η διάκριση των σκοπών ασφαλείας που καλύπτουν πολλαπλούς κινδύνους για την εταιρία και αποτελεί άλλο ένα επικοινωνιακό εργαλείο το οποίο μπορεί να χρησιμοποιήσει ο αναλυτής κατά την διάρκεια της διαδικασίας διαχείρισης κινδύνου.

Στην συνέχεια, στόχος της επόμενης δραστηριότητας του ερευνητή είναι να καθορίσει τα επίπεδα ασφαλείας, όπως αυτά ορίζονται βάσει:

- Της σταθερότητας του μηχανισμού που ικανοποιεί τον σκοπό ασφαλείας
- Το επίπεδο διαβεβαίωσης πως ο μηχανισμός ικανοποιεί τον σκοπό ασφαλείας

Γενικά υπάρχουν τρία επίπεδα αντίστασης τα οποία λαμβάνονται υπόψη. Κάθε ένα από αυτά καθορίζεται από το ποια επίπεδα απειλών είναι ικανά να αντιμετωπίσουν χωρίς να δημιουργηθεί πρόβλημα στο στοιχείο το οποίο καλύπτεται από τον συγκεκριμένο σκοπό ασφαλείας. Τα τρία επίπεδα αντίστασης είναι τα εξής:

- Στοιχειώδες. Ο σκοπός ασφαλείας μπορεί να καλύψει απειλές χαμηλού επιπέδου.
- Μέτριο. Ο σκοπός ασφαλείας μπορεί να καλύψει απειλές μέτριου επιπέδου.
- Υψηλό. Ο σκοπός ασφαλείας μπορεί να καλύψει απειλές υψηλού επιπέδου.

Αν κάποιος σκοπός ασφαλείας καλύπτει πολλαπλές απειλές, ως επίπεδο αντίστασης ορίζουμε αυτό με την υψηλότερη τιμή.

Όσον αφορά τα επίπεδα διαβεβαίωσης, μπορούμε να διακρίνουμε εφτά διακριτά επίπεδα. Τα συγκεκριμένα επίπεδα ορίζονται βάσει κριτηρίων αυξανόμενης σημασίας. Αποτελούν την έκφραση της αυτοπεποίθησης του οργανισμού πως μπορεί να εφαρμόσει τις όποιες προαπαιτήσεις ασφαλείας κληθεί να υλοποιήσει. Σαφώς είναι σημαντικό να αναλογιστούμε το κόστος υλοποίησης καθώς και την ικανότητα του οργανισμού να ανταπεξέλθει στις όποιες ανάγκες εγείρει η εφαρμογή των ζητηθέντων επιπέδων. Ο οργανισμός μπορεί να ορίσει τα δικά του επίπεδα διαβεβαίωσης, όμως τα εφτά ήδη υπάρχοντα επίπεδα καλύπτουν την πλειοψηφία των περιπτώσεων:

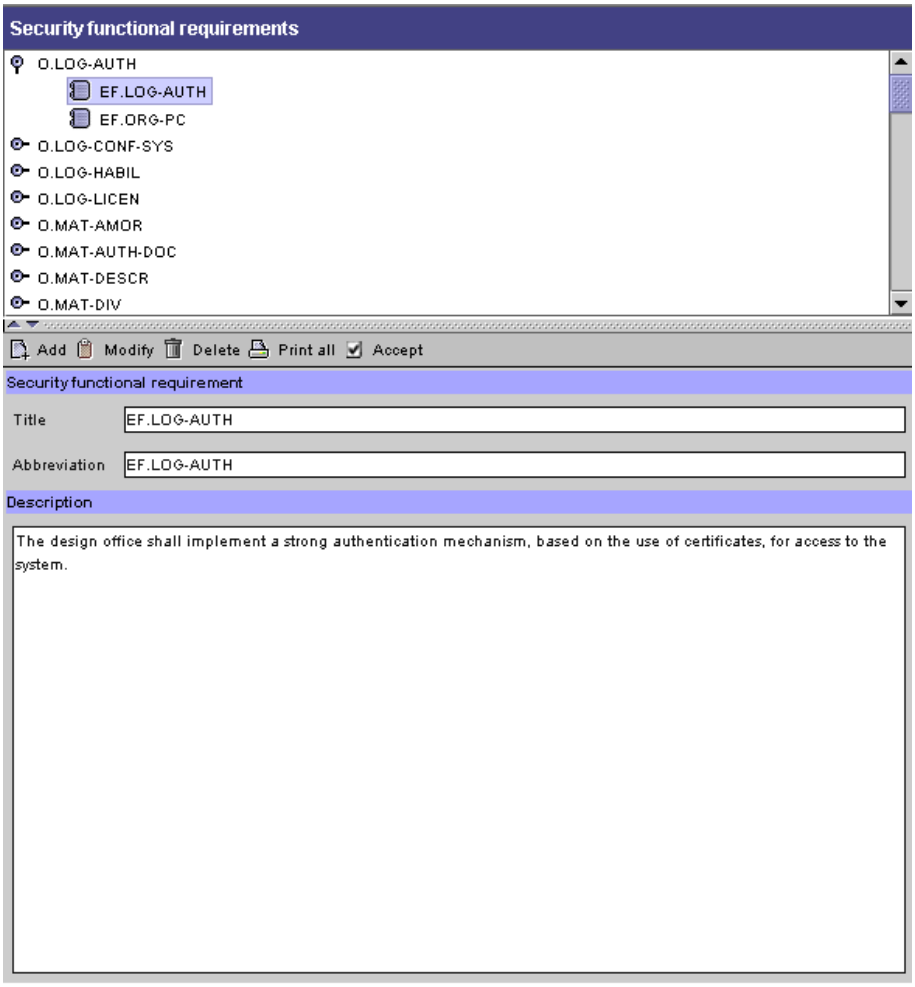
- Δοκιμασμένο λειτουργικά.
- Δοκιμασμένο δομικά.
- Δοκιμασμένο και επιβεβαιωμένο βάσει ορισμένης μεθοδολογίας.
- Δημιουργημένο, δοκιμασμένο και αναθεωρημένο βάσει ορισμένης μεθοδολογίας.
- Δημιουργημένο και δοκιμασμένο από χρήση μερικώς επίσημης μεθόδου.
- Δημιουργημένο και δοκιμασμένο από χρήση πλήρως επίσημης μεθόδου.

3.4.7 Καθορισμός απαιτήσεων ασφαλείας

Η συγκεκριμένη δραστηριότητα, επιτρέπει στον αναλυτή να καθορίσει τις λειτουργικές απαιτήσεις ασφαλείας, καθώς και τις απαιτήσεις διαβεβαίωσης οι οποίες καλύπτουν τους σκοπούς ασφαλείας. Επίσης σε αυτό το στάδιο της διαδικασίας διαχείρισης κινδύνου, ο αναλυτής καλείται να επιδείξει τα επίπεδα κάλυψης των απαιτήσεων ασφαλείας σε σχέση με τους σκοπούς ασφαλείας.

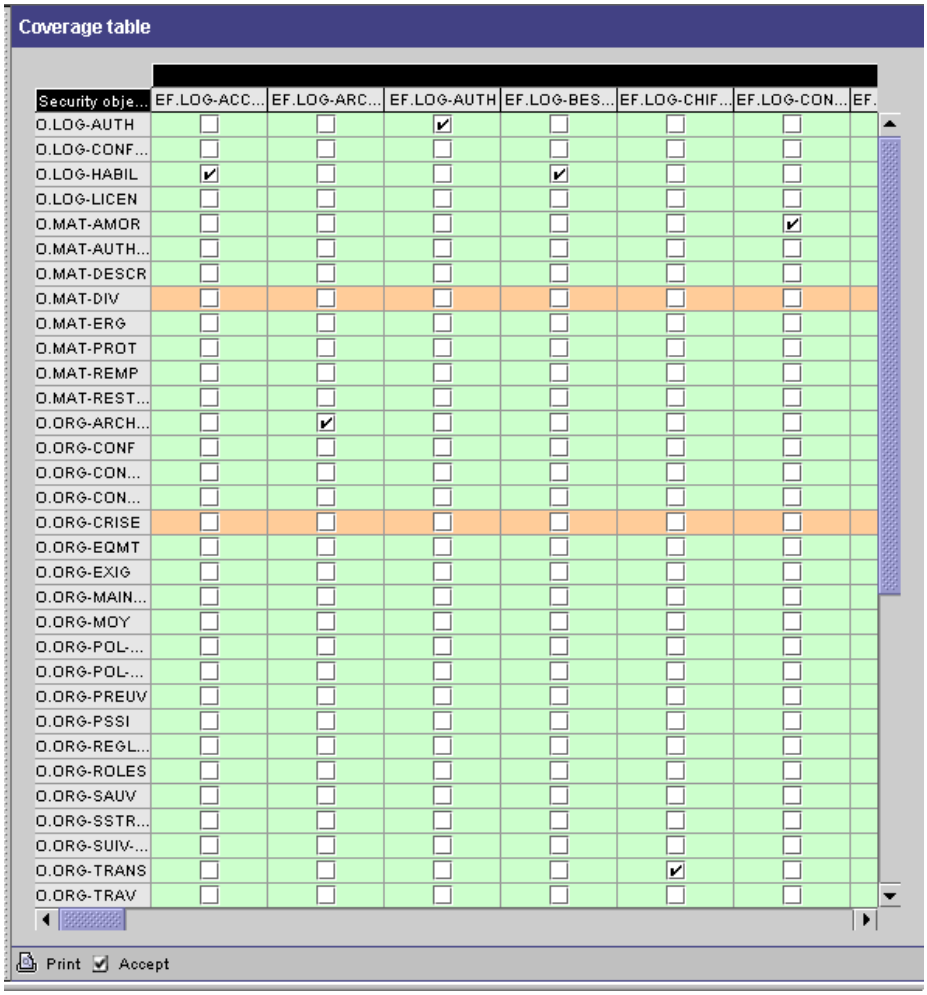
Ο καθορισμός των λειτουργικών απαιτήσεων ασφαλείας, πραγματοποιείται βάσει των καθορισμένων σκοπών ασφαλείας. Για να γίνει ο καθορισμός, είναι απαραίτητο να λάβουμε υπόψη όλη την προηγούμενη πληροφορία που έχουμε συλλέξει. Αυτή η διαδικασία απαιτεί την ύπαρξη συμφωνίας μεταξύ των μέσων που χρησιμοποιούμε για να καθοριστούν οι απαιτήσεις. Μέσα όπως ο προϋπολογισμός της μελέτης ή τεχνικοί περιορισμοί μπορούν να εκτροχιάσουν αυτό το βήμα της όλης διαδικασίας.

Η μεθοδολογία EBIOS προσφέρει για άλλη μια φορά τα κατάλληλα εργαλεία για να μπορέσει ο αναλυτής να καταγράψει τα κατάλληλα μέτρα ασφαλείας. Για κάθε σκοπό ασφαλείας, το πρόγραμμα επιτρέπει στον αναλυτή να καταγράψει διαφορετικά μέτρα ασφαλείας.



ΕΙΚΟΝΑ 21 ΛΕΙΤΟΥΡΓΙΚΕΣ ΑΠΑΙΤΗΣΕΙΣ ΑΣΦΑΛΕΙΑΣ

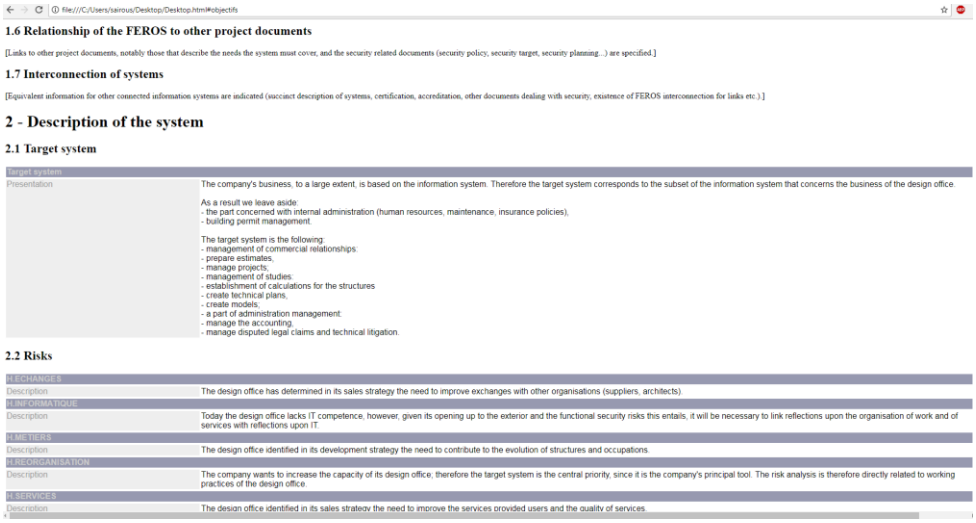
Η EBIOS προσφέρει τον κατάλληλο πίνακα ώστε να συσχετιστούν οι σκοποί ασφαλείας με τις απαιτήσεις ασφαλείας. Μπορείτε να δείτε ένα παράδειγμα τέτοιου πίνακα στην παρακάτω εικόνα.



ΕΙΚΟΝΑ 22 ΣΥΣΧΕΤΙΣΗ ΣΚΟΠΩΝ ΑΣΦΑΛΕΙΑΣ ΜΕ ΑΠΑΙΤΗΣΕΙΣ ΑΣΦΑΛΕΙΑΣ

3.4.8 Παραγωγή αναφοράς

Η EBIOS προσφέρει έναν πολύ βολικό τρόπο να συντάσσεται η αναφορά για την μελέτη που μόλις έχει γίνει. Η διαδικασία είναι πολύ απλή και διαρκεί μόλις λίγα δευτερόλεπτα. Στο κύριο menu του προγράμματος επιλέγουμε την επιλογή “Create summary documents”. Στην συνέχεια επιλέγουμε την μελέτη για την οποία θέλουμε να παραχθεί αναφορά και κάνουμε click στο κουμπί generate. Αποτέλεσμα αυτών των ενεργειών είναι η δημιουργία μίας HTML σελίδας η οποία περιέχει την αναλυτική αναφορά της μελέτης και ενός επιπλέον φακέλου ο οποίος έχει όλα τα βοηθητικά αρχεία που χρειάζεται η αναφορά πχ. φωτογραφίες διαγραμμάτων που εμφανίζονται στην αναφορά.



1.6 Relationship of the FEROS to other project documents

[Links to other project documents, notably those that describe the needs the system must cover, and the security related documents (security policy, security target, security planning...) are specified.]

1.7 Interconnection of systems

[Equivalent information for other connected information systems are indicated (succinct description of systems, certification, accreditation, other documents dealing with security, existence of FEROS interconnection for links etc.).]

2 - Description of the system

2.1 Target system

Target system	
Presentation	The company's business, to a large extent, is based on the information system. Therefore the target system corresponds to the subset of the information system that concerns the business of the design office. As a result we leave aside: - the part concerned with internal administration (human resources, maintenance, insurance policies), - building permit management. The target system is the following: - management of commercial relationships: - prepare estimates, - manage projects, - management of studies: - establishment of calculations for the structures - create technical plans, - create models; - a part of administration management: - manage the accounting; - manage disputed legal claims and technical litigation.

2.2 Risks

R.ECHANGES	
Description	The design office has determined in its sales strategy the need to improve exchanges with other organisations (suppliers, architects).
R.INFORMATIQUE	
Description	Today the design office lacks IT competence, however, given its opening up to the exterior and the functional security risks this entails, it will be necessary to link reflections upon the organisation of work and of services with reflections upon IT.
R.METIERS	
Description	The design office identified in its development strategy the need to contribute to the evolution of structures and occupations.
R.REORGANISATION	
Description	The company wants to increase the capacity of its design office, therefore the target system is the central priority, since it is the company's principal tool. The risk analysis is therefore directly related to working practices of the design office.
R.SERVICES	
Description	The design office identified in its sales strategy the need to improve the services provided users and the quality of services.

ΕΙΚΟΝΑ 23 ΑΝΑΦΟΡΑ EBIOS

Κεφάλαιο 4

Secure Tropos

4.1 Εισαγωγή

Η ασφαλής σχεδίαση πληροφοριακών συστημάτων, αποσκοπεί σε αξιόπιστα συστήματα τα οποία δεν επηρεάζονται από οποιαδήποτε πηγή κακόβουλων ενεργειών, ανθρώπινων λαθών και αστοχίας υλικού. (14) Η διαδικασία της ασφάλισης ενός συστήματος, είναι ένας συμβιβασμός μεταξύ των απαιτήσεων ασφαλείας που έχουν καθοριστεί από τον αναλυτή ρίσκου και κατ' επέκταση από τον υπεύθυνο οργανισμό και των λειτουργικών απαιτήσεων που θα πρέπει να πληροί το πληροφοριακό σύστημα. Οι απαιτήσεις ασφαλείας συγκαταλέγονται ανάμεσα στις επονομαζόμενες μη-λειτουργικές απαιτήσεις του πληροφοριακού συστήματος και ορίζονται ως η εκδήλωση μίας υψηλού επιπέδου πολιτικής ασφαλείας σε λεπτομερείς απαιτήσεις ενός πληροφοριακού συστήματος.

Σε αντίθεση με μη λειτουργικές απαιτήσεις όπως η αξιοπιστία ή η επίδοση ενός συστήματος για τις οποίες οι σχεδιαστές συστημάτων έχουν φροντίσει να ληφθούν υπόψη κατά την σχεδίαση του συστήματος, οι πιθανές απαιτήσεις ασφαλείας εντάσσονται με το υπόλοιπο σύστημα εφόσον αυτό έχει ήδη ολοκληρωθεί και όχι κατά την αρχική περίοδο σχεδίασής του. Αποτέλεσμα αυτής της πρακτικής των σχεδιαστών, είναι η εμφάνιση αδυναμιών στο πληροφοριακό σύστημα μιας και η εφαρμογή των μέτρων ασφαλείας που μπορούν να ικανοποιήσουν τις απαιτήσεις ασφαλείας, ορισμένες φορές απαιτούν σημαντικούς ανασχεδιασμούς του συστήματος. Καθ' αυτό τον τρόπο, μπορεί πολλές φορές να δημιουργούνται συστήματα τα οποία δεν έχουν πλήρως ενσωματωμένα και εναρμονισμένα μέτρα ασφαλείας με τις υπόλοιπες λειτουργίες τους. Το γεγονός αυτό, σε συνδυασμό με τα περιορισμένα χρονοδιαγράμματα που αφορούν την ολοκλήρωση και παράδοση του πληροφοριακού συστήματος, μας οδηγεί σε συστήματα τα οποία όχι μόνο είναι ευάλωτα και ημιτελή εξ ορισμού από την πρώτη στιγμή που θα παραδοθούν, μπορεί ακόμα και να είναι ευάλωτα εν γνώσει των σχεδιαστών του.

Πιστεύουμε πως είναι πλέον σαφής η ανάγκη της ενσωμάτωσης των μέτρων ασφαλείας σε αρχικό στάδιο της σχεδίασης του συστήματος. Για να μπορέσουν οι σχεδιαστές συστημάτων να λάβουν υπόψη τους τα μέτρα ασφαλείας κατά την περίοδο της σχεδίασης του συστήματος και να μπορέσουν επίσης να τα ενσωματώσουν στο σύστημα εγκαίρως χρειάζονται μία μεθοδολογία η οποία θα τους παρέχει τα κατάλληλα εργαλεία για αυτού του είδους την διαδικασία.

Η αρχική ιδέα ήταν να χρησιμοποιηθεί ο πρακτοροστραφής τρόπος σχεδίασης συστημάτων. Ο συγκεκριμένος τρόπος στηρίζεται στην ιδέα διάφορων οντοτήτων μέσα στο πληροφοριακό σύστημα, οι οποίες παρέχουν μια προκαθορισμένη υπηρεσία και ο συνδυασμός τους συντελεί το πληροφοριακό σύστημα. Από τον ορισμό και μόνο μπορούμε να δούμε πως ο συγκεκριμένος τρόπος έχει πολλές προοπτικές ώστε να καλύψει τις ανάγκη του σχεδιαστή να συμπεριληφθούν οι απαιτήσεις ασφαλείας στο σύστημα. Η επιτυχημένη ενσωμάτωση των απαιτήσεων ασφαλείας καθ' αυτό τον τρόπο, απαιτεί τα υπόλοιπα υποσυστήματα να λαμβάνουν υπόψη τους τα συστήματα που είναι υπεύθυνα για την ασφάλεια του πληροφοριακού συστήματος και να μην τα παρακάμπτουν για οποιοδήποτε λόγο. Παρόλα αυτά, οι μεθοδολογίες που καλύπτουν την πρακτοροστραφή μεθοδολογία σχεδίασης πληροφοριακών συστημάτων, δεν καλύπτουν τις απαιτούμενες προδιαγραφές ώστε να παρέχουν τα

απαραίτητα εργαλεία που μπορεί να χρειαστεί ένας σχεδιαστής. Κοινώς, αδυνατούν να προσφέρουν μία επαρκής ασφαλειοστραφή μεθοδολογία σχεδίασης πληροφοριακών συστημάτων.

4.2 Tropos

Στο (15) παρουσιάζεται η μεθοδολογία Secure Tropos, η οποία καλύπτει τα όποια κενά μπορεί να υπήρχαν στην πρακτοροστραφή προσέγγιση του προβλήματος της σχεδίασης ασφαλών συστημάτων. Η μεθοδολογία στηρίζεται στην Tropos (16), συνεπώς μπορούμε να πούμε πως η Secure Tropos αποτελεί επέκταση της μεθοδολογίας Tropos. Η απόφαση των συγγραφέων να στηριχθούν στην Tropos και να μην δημιουργήσουν μία εντελώς καινούρια μεθοδολογία, δικαιολογείται από το γεγονός πως η Tropos παρείχε εργαλεία τα οποία ήταν ήδη γνώριμα από τους σχεδιαστές πληροφοριακών συστημάτων όπως η γλώσσα UML. Επίσης, η έννοια της ασφάλειας δεν ήταν εντελώς άγνωστος όρος για την Tropos, συνεπώς οι τροποποιήσεις που θα χρειαζόντουσαν για να δημιουργηθεί η Secure Tropos ήταν λιγοστές. Η Tropos υιοθετεί το πλαίσιο μοντελοποίησης i*, στο οποίο χρησιμοποιεί έννοιες όπως:

- Πράκτορας
- Στόχος
- Προαπαιτήσεις / Εξαρτήσεις
- Ρόλος
- Θέση
- Έργο
- Πόρος
- Ικανότητα
- Εξαρτώμενος
- Εξαρτηθέντας

Κρίνοντας από τους όρους που χρησιμοποιεί η Tropos, μπορούμε να καταλήξουμε στο συμπέρασμα πως το πληροφοριακό σύστημα, προβάλλεται από την Tropos ως ένας συνδυασμός πρακτόρων με ορισμένους στόχους και ρόλους, οι οποίοι εξαρτώνται πολλές φορές από άλλους πράκτορες εντός του συστήματος προκειμένου να πραγματοποιήσουν τους στόχους τους και να εκπληρώσουν τους ρόλους τους.

Ως πράκτορα ορίζουμε την οντότητα την οποία έχει σκοπό και στρατηγικούς στόχους εντός του πληροφοριακού συστήματος.

Ως ρόλο, ορίζουμε τον αφαιρετικό χαρακτηρισμό της συμπεριφοράς ενός πράκτορα εντός του πληροφοριακού συστήματος.

Η θέση ενός πράκτορα στο πληροφοριακό σύστημα, ορίζεται ως το σύνολο των ρόλων τους οποίους καλείται να εκπληρώσει ένας πράκτορας του πληροφοριακού συστήματος.

Η Tropos χωρίζει τον όρο στόχος σε δύο υποκατηγορίες. Τους σκληρούς στόχους και τους μαλακούς στόχους. Οι σκληροί στόχοι, αντικατοπτρίζουν μία συνθήκη την οποία ένας πράκτορας καλείται να πραγματοποιήσει ήτοι τους στρατηγικούς στόχους ενός πράκτορα στο πληροφοριακό σύστημα. Ο όρος μαλακός στόχος, ορίζεται από την Tropos ως ένα εργαλείο προκειμένου να αντιληφθεί ο χρήστης της, τις μη λειτουργικές απαιτήσεις του πληροφοριακού συστήματος. Για παράδειγμα, η έκφραση “το σύστημα πρέπει να είναι επεκτάσιμο” χαρακτηρίζεται ως μαλακός στόχος.

Το έργο, εκπροσωπεί σε ένα υψηλό, αφαιρετικό επίπεδο τον τρόπο με τον οποίο γίνεται κάτι. Η εκπλήρωση ενός έργου μπορεί να είναι το μέσο με το οποίο πραγματοποιείται η εκπλήρωση ενός μαλακού στόχου. Μπορούμε να μοντελοποιήσουμε διαφορετικά έργα προς επίτευξη ενός

Σχόλιο [C8]: Depender. Δεν με νοιαζει καθολου, λες και θα την διαβασει ποτε κανεις την εργασια.

Σχόλιο [C9]: Αντι να καθομαι να παιζω μηχανηματα που με εχει βαλει να παιξω η Greunion, καθομαι και γραφω HTOI. HTOI!

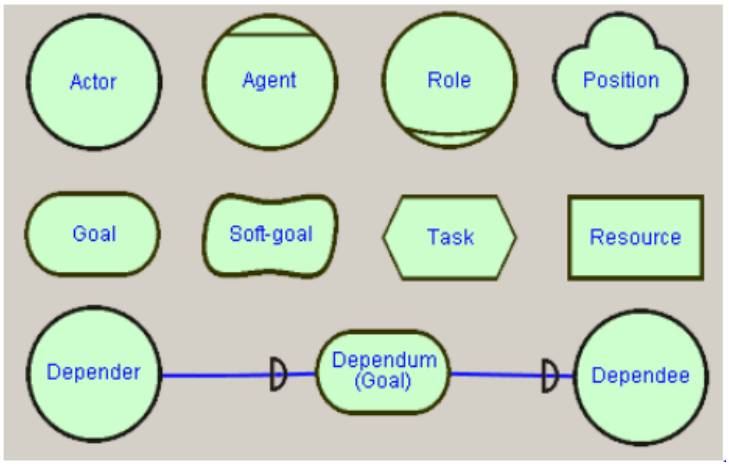
Σχόλιο [C10]: Αντιγραφή επικόλληση για την παρουσίαση :’D

συγκεκριμένου στόχου και να επιλέξουμε αυτόν που θα κρίνουμε καλύτερο βάσει προκαθορισμένων κριτηρίων.

Ως πόρο, μπορούμε να ορίσουμε την φυσική ή πληροφοριακής φύσης οντότητα την οποία χρειάζεται ένας πράκτορας. Αυτό που μας απασχολεί κυρίως με τους πόρους είναι το αν είναι διαθέσιμος ένας πόρος όταν τον χρειαζόμαστε και ποια είναι η υπεύθυνη οντότητα για αυτό τον πόρο.

Μία εξάρτηση ή αλλιώς προ απαίτηση μεταξύ δύο διαφορετικών πρακτόρων υφίσταται όταν ο ένας εκ των δύο πρακτόρων εξαρτάται από έναν άλλο πράκτορα. Η εξάρτηση μπορεί να αφορά την εκπλήρωση ενός έργου, εκπλήρωση στόχου ή παράδοση κάποιου πόρου.

Ο όρος ικανότητα εκφράζει την ικανότητα ενός πράκτορα να επιλέξει και να εκπληρώσει ένα έργο προς γενικότερη εκπλήρωση ενός στόχου, δεδομένου ότι υφίστανται προκαθορισμένοι όροι και έχουν εκπληρωθεί οι όποιες προαπαιτήσεις επιβάλλονται. Στην παρακάτω εικόνα μπορούμε να δούμε την γραφική αναπαράσταση των όρων που μόλις περιγράψαμε, όπως αυτοί χρησιμοποιούνται από την μεθοδολογία.



ΕΙΚΟΝΑ 24 ΓΡΑΦΙΚΗ ΑΝΑΠΑΡΑΣΤΑΣΗ ΟΡΩΝ ΤΗΣ TROPOS

Η Tropos (17) καλύπτει τις πέντε κύριες φάσεις ανάπτυξης ενός πληροφοριακού συστήματος οι οποίες είναι οι εξής:

- Πρώιμη ανάλυση απαιτήσεων.
- Ύστερη ανάλυση απαιτήσεων.
- Αρχιτεκτονική σχεδίαση.
- Λεπτομερής σχεδίαση.
- Ανάπτυξη συστήματος

Στην Tropos, η πρώιμη ανάλυση απαιτήσεων αφορά την αναγνώριση και ανάλυση των ενδιαφερόντων μερών και των προθέσεών τους. Τα ενδιαφερόμενα μέρη μοντελοποιούνται ως κοινωνικοί πράκτορες οι οποίοι εξαρτούνται από άλλους πράκτορες εντός του συστήματος ώστε να επιτευχθούν στόχοι, να εφαρμοστούν σχέδια και να υπάρχουν διαθέσιμοι πόροι. Οι προθέσεις του κάθε πράκτορα μοντελοποιούνται ως στόχοι και έπειτα από σχετική μελέτη, μετατρέπονται σε πιο καλοδουλεμένους στόχους οι οποίοι μπορούν να υποστούν αξιολόγηση από τρίτους.

Η ύστερη ανάλυση απαιτήσεων, πάντα βάσει της Tropos, εστιάζει στο εν τη γενέσει πληροφοριακό σύστημα και στην κατάσταση στην οποία θα βρίσκεται μετά την ολοκλήρωσή του. Σε αυτό το στάδιο αναγνωρίζονται τυχόν εξαρτήσεις μεταξύ πρακτόρων και διαδικασίες που θα πρέπει να εκτελούνται από τους πράκτορες του συστήματος. Το ίδιο το πληροφοριακό σύστημα παρουσιάζεται ως ένας πράκτορας μέσα στον ευρύτερο οργανισμό και αναγνωρίζονται οι εξαρτήσεις που έχει ο οργανισμός από το πληροφοριακό σύστημα, καθώς και τις εξαρτήσεις του πληροφοριακού συστήματος από τον οργανισμό.

Σχόλιο [C11]: Καταντάω γραφικός, αλλά ΧΑ-ΡΑ-ΜΙ-ΖΟ-ΜΑΙ

Η αρχιτεκτονική σχεδίαση του συστήματος πρόκειται για την φάση σχεδίασης κατά την οποία, ορίζουμε το σύστημα ως το συνονθύλευμα των πρακτόρων που το αποτελούν και εξετάζουμε επί μέρους κάθε πράκτορα που το αποτελεί, καθώς και τις ροές δεδομένων μεταξύ των πρακτόρων του πληροφοριακού συστήματος. Η συγκεκριμένη φάση αποτελείται από τέσσερεις διαφορετικές διεργασίες:

- Την αναγνώριση των πρακτόρων
- Προσθήκη νέων πρακτόρων
- Τον καθορισμό των στόχων και των ικανοτήτων του κάθε πράκτορα
- Την κατηγοριοποίηση του κάθε πράκτορα βάσει των ικανοτήτων του και ανάθεση κατάλληλων ευθυνών.

Η τελευταία φάση σχεδιασμού του συστήματος, πριν προχωρήσουμε στην ανάπτυξη του ίδιου του συστήματος είναι η φάση της λεπτομερούς σχεδίασης. Κατά την διάρκεια αυτής της φάσης οι κατασκευαστές του συστήματος, ορίζουν επακριβώς το πως θα εφαρμοστούν οι στόχοι και οι ικανότητες των πρακτόρων που έχουν αναγνωριστεί από την προηγούμενη φάση. Αν για παράδειγμα έχουμε αναγνωρίσει σε προηγούμενη φάση πως ένας πράκτορας του συστήματος οφείλει να έχει ικανότητες throttling, σε αυτή την φάση θα πρέπει να οριστεί το πως θα εφαρμοστεί και ποια θα είναι η έκταση της εφαρμογής αυτού του πράκτορα.

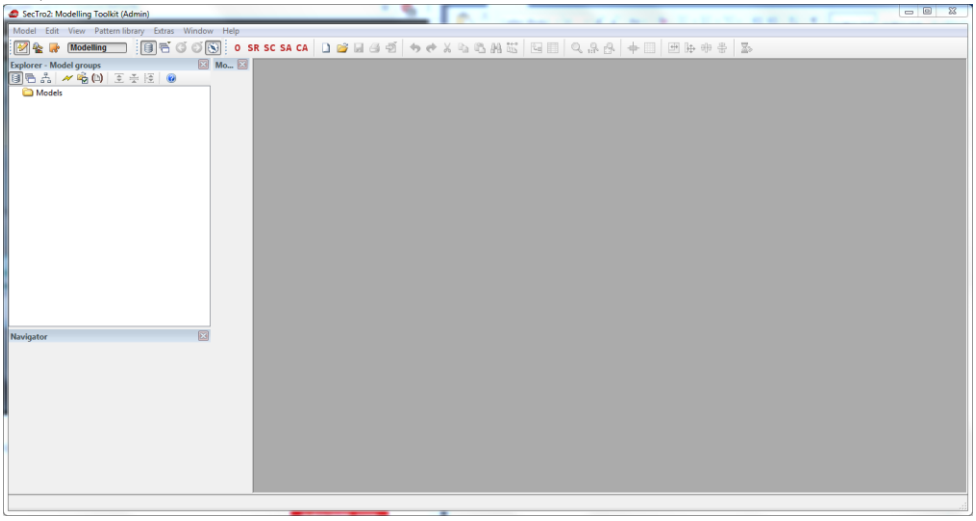
4.3 Secure Tropos και SecTro

Η Secure Tropos είναι επέκταση της μεθοδολογίας Tropos την οποία και αναλύσαμε στην προηγούμενη ενότητα. Χρησιμοποιεί τις ίδιες έννοιες και αρχές με την Tropos, με μόνη διαφορά ότι το πραγματοποιεί υπό ένα πρίσμα το οποίο ευνοεί την ασφάλεια του συστήματος. Επιπλέον, η Secure Tropos αποτελείται από τις ίδιες διαδικασίες ανάπτυξης συστήματος όπως και η Secure Tropos.

Προς εφαρμογή της Secure Tropos, κατασκευάστηκε το εργαλείο SecTro (18). Το SecTro είναι μια εφαρμογή γραμμένη σε Java, με την οποία ο αναλυτής του συστήματος μπορεί να χρησιμοποιήσει το διατιθέμενο notation της SecTropos, το οποιο θα εξετάσουμε σε μία από τις επόμενες παραγράφους, ώστε να σχεδιάσει ένα σύστημα.

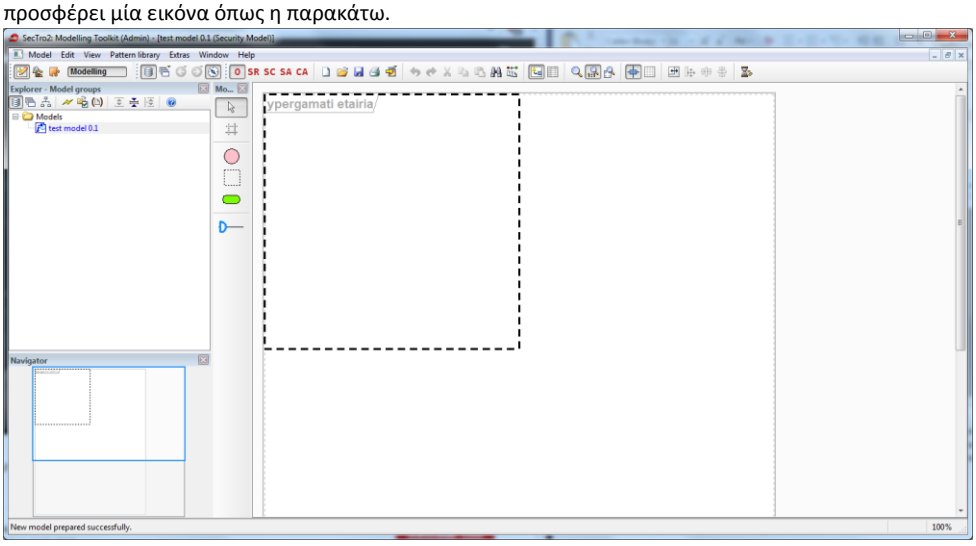
Η εγκατάσταση του εργαλείου είναι σχετικά εύκολη, καθώς στο διατιθέμενο πακέτο, συμπεριλαμβάνεται και η απαραίτητη έκδοση βάσης δεδομένων που απαιτείται από το εργαλείο ώστε να δουλέψει. Να σημειώσουμε πως πρώτα πρέπει να εγκατασταθεί η βάση δεδομένων και να δώσουμε ιδιαίτερη προσοχή στον λογαριασμό διαχειριστή της βάσης δεδομένων, μιας και θα χρειαστεί να το εισάγουμε κατά την εγκατάσταση του εργαλείου SecTro. Εφόσον καταφέρουμε να το εγκαταστήσουμε και να το τρέξουμε, θα αντικρίσουμε την κεντρική οθόνη του εργαλείου, όπως εμφανίζεται στην

επόμενη εικόνα.



ΕΙΚΟΝΑ 25 ΚΕΝΤΡΙΚΗ ΟΘΟΝΗ SECTRO

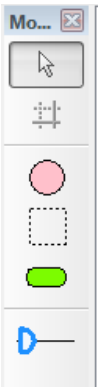
Για να αρχίσουμε να χρησιμοποιούμε το εργαλείο, χρειάζεται να δημιουργήσουμε ένα μοντέλο συστήματος που θέλουμε να αναπαραστήσουμε. Επιλέγοντας την επιλογή Model -> New και εισάγοντας τα απαραίτητα δεδομένα, όπως π.χ. το όνομα του συστήματος, το εργαλείο θα μας προσφέρει μία εικόνα όπως η παρακάτω.



ΕΙΚΟΝΑ 26 ΚΑΜΒΑΣ SECTRO

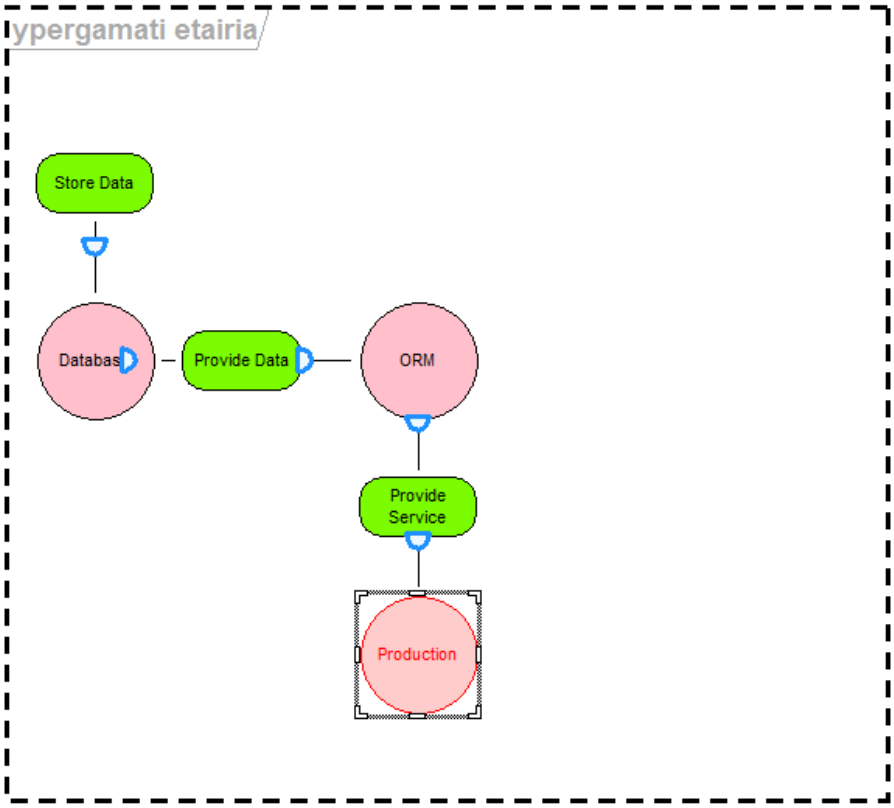
Το συγκεκριμένο παράθυρο, αποτελεί την κύρια οθόνη του προγράμματος το οποίο θα ονομάσουμε καμβά. Πάνω στον καμβά, ο αναλυτής μπορεί να αναπαραστήσει το σύστημα χρησιμοποιώντας τα

διάφορα εργαλεία της SecTro. Ο καμβάς της SecTro έχει πολλαπλά παράθυρα. Το παράθυρο που απεικονίζεται στην παραπάνω εικόνα είναι η απεικόνιση του οργανισμού. Σε αυτό το παράθυρο μπορούμε να κατασκευάσουμε μία αρχιτεκτονική άποψη του συστήματός μας. Τα προσφερόμενα εργαλεία παραθέτονται στην παρακάτω εικόνα.



ΕΙΚΟΝΑ 27 ΕΡΓΑΛΕΙΑ ΑΡΧΙΤΕΚΤΟΝΙΚΗΣ ΑΠΟΨΗΣ

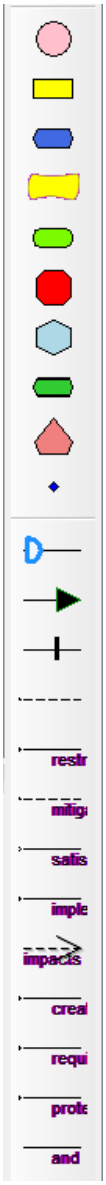
Ο ροζ κύκλος χρησιμοποιείται για να αναπαραστήσει τους πράκτορες του συστήματος. Επιπλέον κάνοντας διπλό κλικ πάνω στο σχήμα εφόσον το τοποθετήσουμε στον καμβά, μπορούμε να παραμετροποιήσουμε στοιχεία που αφορούν τον συγκεκριμένο πράκτορα, όπως π.χ. το όνομά του. Το επόμενο εργαλείο μας βοηθά να σχεδιάσουμε επιπλέον οργανισμούς εφόσον εμείς το κρίνουμε απαραίτητο. Το πράσινο σχήμα αναπαριστά τους στόχους του συστήματος και το επόμενο σύμβολο με το μπλε τρίγωνο και την γραμμή χρησιμοποιείται για να οριστούν οι εξαρτήσεις μεταξύ των πρακτόρων του συστήματος.



ΕΙΚΟΝΑ 28 ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΑΠΟΨΗ ΣΥΣΤΗΜΑΤΟΣ

Το παραπάνω σχήμα, μεταφράζεται ως εξής. Ο πράκτορας Database έχει ως στόχο να αποθηκεύει δεδομένα, ο πράκτορας ORM έχει ως στόχο να παρέχει δεδομένα και ο πράκτορας Production έχει ως στόχο να παρέχει κάποια υπηρεσία. Ταυτόχρονα μπορούμε να δούμε και τις εξαρτήσεις μεταξύ των πρακτόρων οι οποίες είναι οι εξής. Ο πράκτορας Production εξαρτάται από τον πράκτορα ORM ώστε να παρέχει υπηρεσίες και ο πράκτορας ORM εξαρτάται από τον πράκτορα Database ώστε να μπορεί να παρέχει δεδομένα.

Το επόμενο παράθυρο του εργαλείου SecTro είναι αυτό το οποίο μας επιτρέπει να θέσουμε απαιτήσεις ασφαλείας καθώς και μέτρα ασφαλείας τα οποία θα σχετίζονται με το σύστημα και θα ικανοποιούν τις απαιτήσεις ασφαλείας. Ορισμένα από τα εργαλεία παραμένουν ίδια με τα εργαλεία του παραθύρου κατασκευής αρχιτεκτονικής άποψης.



ΕΙΚΟΝΑ 29 ΕΡΓΑΛΕΙΑ ΠΡΟΒΟΛΗΣ SECURITY REQUIREMENTS

Ορισμένα από αυτά τα εργαλεία τα είδαμε στην προηγούμενη ενότητα και συνεπώς δεν θα τα αναλύσουμε περαιτέρω.

 Αυτό το εργαλείο χρησιμοποιείται για να απεικονιστεί ο όρος πόρος. Με τον όρο πόρο μπορούμε να χαρακτηρίσουμε κυρίως δεδομένα που διέρχονται, πηγάζουν ή καταλήγουν στο σύστημα. Επίσης πόροι μπορούν να χαρακτηρισθούν και οι χρήστες του συστήματος.

 Το συγκεκριμένο εικονίδιο αναπαριστά τον συγκεκριμένο τρόπο με τον οποίο πραγματοποιείται ένας στόχος

 Εικονίδιο μαλακού στόχου.

 Εικονίδιο περιορισμού ασφαλείας. Οι περιορισμοί ασφαλείας απεικονίζουν τις ενέργειες τις οποίες δεν θα πρέπει το σύστημα να πραγματοποιηθούν.

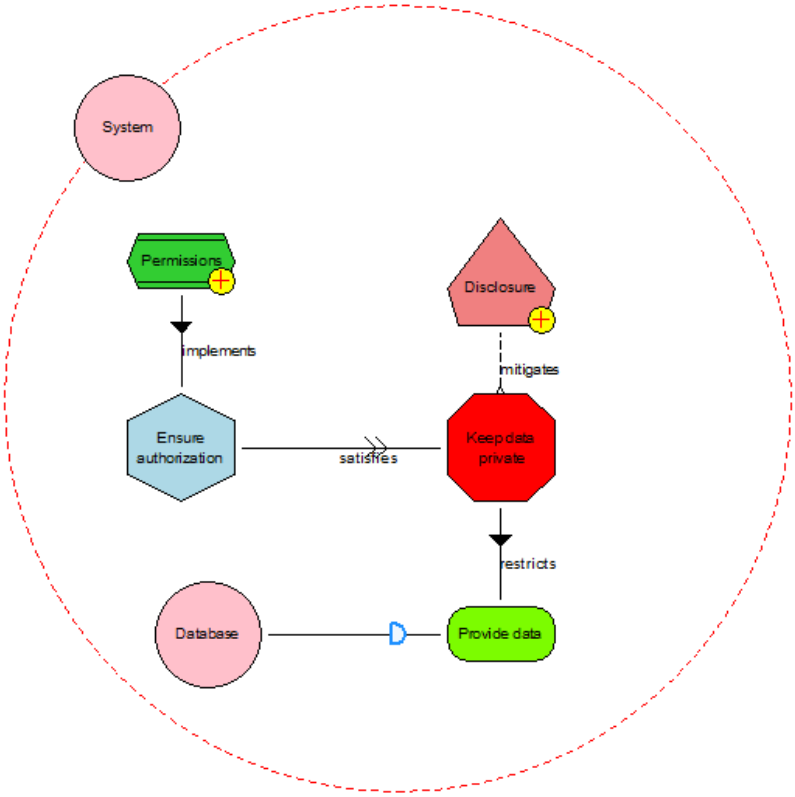
 Εικονίδιο σκοπού ασφαλείας. Ο σκοπός ασφαλείας εκπροσωπεί μία γενική και αφαιρετική άποψη των μέτρων που πρέπει να εφαρμοστούν ώστε να ικανοποιηθεί ένας περιορισμός ασφαλείας.

 Εικονίδιο μηχανισμού ασφαλείας. Το συγκεκριμένο εικονίδιο απεικονίζει την πραγματική τεχνική λύση η οποία μπορεί να ικανοποιεί κάποιο σκοπό ασφαλείας.

 Το συγκεκριμένο εικονίδιο απεικονίζει κάποια απειλή από την οποία μπορεί να κινδυνεύει το σύστημα. Συνήθως οι απειλές έχουν αναγνωριστεί κατά την φάση της διαδικασίας διαχείρισης κινδύνου.

 Το εικονίδιο της λογικής πράξης και.

Τα υπόλοιπα εικονίδια χρησιμοποιούνται για να ενώσουν τα παραπάνω εικονίδια τα οποία αναλύσαμε. Αναλόγως την φύση της σχέσης μεταξύ δύο εικονιδίων, χρησιμοποιούμε το κατάλληλο εικονίδιο συσχέτισης.



ΕΙΚΟΝΑ 30 ΑΠΑΙΤΗΣΕΙΣ ΑΣΦΑΛΕΙΑΣ

Η παραπάνω εικόνα ερμηνεύεται ως εξής. Το πληροφοριακό μας σύστημα αποτελείται από μία βάση δεδομένων. Στόχος της βάσης δεδομένων είναι να παρέχει δεδομένα σε όποιον τα ζητήσει. Στο σύστημα επίσης υπάρχει και η απειλή της διαρροής των δεδομένων, κάτι το οποίο μας αναγκάζει να θέσουμε μία απαίτηση ασφαλείας η οποία θα ορίζει πως θέλουμε τα δεδομένα να μην είναι προσπελάσιμα από μη εξουσιοδοτημένους χρήστες. Η συγκεκριμένη απαίτηση ικανοποιείται από τον σκοπό ασφαλείας ο οποίος αφορά την εξουσιοδότηση χρηστών και ο μηχανισμός με τον οποίο έχουμε επιλέξει να εφαρμόσουμε την εξουσιοδότηση των χρηστών, είναι μέσω ενός μηχανισμού δικαιωμάτων χρηστών.

Η άνοδος των νεφοϋπολογιστικών συστημάτων οδήγησε τους προγραμματιστές τις SecTro να δημιουργήσουν ένα feature στο πρόγραμμα ώστε να ικανοποιηθεί η ανάγκη ανάλυσης αυτών των συστημάτων. Γνώμη του συγγραφέα είναι πως η συγκεκριμένη ανάγκη μπορούσε να καλυφθεί με τα ήδη υπάρχοντα εργαλεία που προσφέρει η SecTro. Παρόλα αυτά, παρακάτω θα εξετάσουμε τα ξεχωριστά εργαλεία που προσφέρει η SecTro.

ΕΙΚΟΝΑ 31 ΕΡΓΑΛΕΙΑ ΑΝΑΛΥΣΗΣ ΝΕΦΟΥΠΟΛΟΓΙΣΤΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Όπως μπορείτε να δείτε, τα εργαλεία που προσφέρει για ανάλυση νεφοϋπολογιστικών συστημάτων είναι ως επί το πλείστον εργαλεία τα οποία έχουμε συναντήσει και αναλύση σε προηγούμενες ενότητες. Το μοναδικό εργαλείο το οποίο είναι διαφορετικό, όχι πραγματικά διαφορετικό όμως όπως θα αντιληφθείτε στις επόμενες γραμμές, είναι το σύμβολο  . Το συγκεκριμένο σύμβολο μοιάζει με το σύμβολο του πράκτορα που έχουμε συναντήσει και η ερμηνεία του είναι σχεδόν η ίδια, μιας και χρησιμοποιείται για να αντιπροσωπεύσει τον πράκτορα νεφοϋπολογιστικού συστήματος. Η λογική κατασκευής και ανάλυσης νεφοϋπολογιστικών συστημάτων είναι ίδια με αυτή που έχουμε συναντήσει στις προηγούμενες ενότητες.

Κεφάλαιο 5

Pris

5.1 Εισαγωγή

Η Secure Tropos κατάφερε να καλύψει το κενό ανάμεσα στο requirements engineering και στις απαιτήσεις ασφαλείας σε εξαιρετικό βαθμό προσφέροντας στην κοινότητα το εργαλείο SecTro. Με την SecTro, οι αναλυτές λογισμικού κατάφεραν να ενσωματώσουν τις όποιες απαιτήσεις ασφαλείας είχανε, στο εκάστοτε αναλυθέν σύστημα.

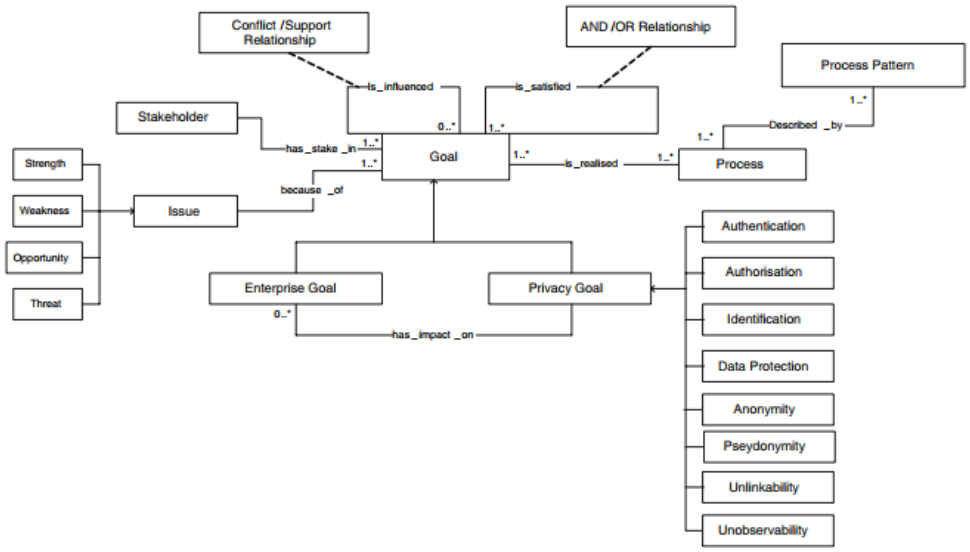
Αυτό που απέτυχε να επιτύχει η Secure Tropos και καθ' επέκταση το εργαλείο SecTro, ήταν να αναγνωρίσει την ιδιωτικότητα ως ξεχωριστή οντότητα από την ασφάλεια. Ωστόσο οι Γκρίτζαλης (19), Koorn (20), Καλλονιάτης (21), υποστήριξαν ο καθένας ξεχωριστά την ιδέα της απόσχισης της ιδιωτικότητας από την ασφάλεια. Έτσι η ιδιωτικότητα έπαψε να είναι υποσύνολο της ασφάλειας και απέκτησε ισχυρότερη υπόσταση στον ακαδημαϊκό χώρο.

Συνεπώς γεννήθηκε η ανάγκη ανάπτυξης μίας μεθοδολογίας η οποία θα κάλυπτε τις όποιες απαιτήσεις ιδιωτικότητας θα μπορούσε να έχει ένα πληροφοριακό σύστημα. Στο (21) οι Καλλονιάτης, Καβακλή και Γκρίτζαλης, παρουσιάζουν την μεθοδολογία Pris, η οποία αναπτύχθηκε για να καλύψει ακριβώς αυτό το κενό που υπήρχε στην σχεδίαση πληροφοριακών συστημάτων.

5.2 Η μέθοδος Pris

Η μέθοδος Pris όπως και η Secure Tropos, αντιλαμβάνεται τις απαιτήσεις του συστήματος ως τους επιθυμητούς στόχους που επιθυμούν τα ενδιαφερόμενα μέρη να επιτευχθούν από το πληροφοριακό σύστημα. Οι στόχοι συνδέονται με ζητήματα που αφορούν το πληροφοριακό σύστημα και πραγματοποιούνται από διαδικασίες. Ως εδώ, η μεθοδολογία Pris μοιάζει με την Secure Tropos ως προς τις γενικές οντότητες πάνω στις οποίες στηρίζονται οι δύο μεθοδολογίες.

Κάπου εδώ όμως τελειώνουν οι ομοιότητες και αρχίζουν οι διαφορές, οι οποίες ομολογουμένως είναι αρκετές. Η Pris εισάγει την συσχέτιση μεταξύ των στόχων μέσω σχέσεων AND/OR, υποστηρίζοντας πως οι στόχοι ενός συστήματος μεταξύ τους μπορεί να συνδυάζονται ώστε να ολοκληρωθούν επιτυχώς ή ακόμα και να έρχονται σε σύγκρουση μεταξύ τους. Επίσης εισάγει τις απαιτήσεις ιδιωτικότητας ως έναν ειδικό τύπο στόχου του πληροφοριακού συστήματος. Ο λόγος που λογίζονται ως στόχοι και οι απαιτήσεις ιδιωτικότητας είναι πιθανώς για να μπορέσουμε να εφαρμόσουμε συσχετίσεις μεταξύ τους αλλά και μεταξύ στόχου πληροφοριακού συστήματος και απαίτησης ιδιωτικότητας. Από τις δύο αυτές διαφορετικές συσχετίσεις που υφίστανται, δημιουργείται ένας νέος τρόπος σύνδεσης τον οποίο η Pris ονομάζει "Επηρεάζει".



ΕΙΚΟΝΑ 32 ΟΝΤΟΤΗΤΕΣ ΚΑΙ ΣΧΕΣΕΙΣ ΤΗΣ PRIS

Όπως μπορείτε να δείτε και στην παραπάνω εικόνα έχουν χωριστεί οι στόχοι σε δύο επιμέρους οντότητες. Τους στόχους ιδιωτικότητας και τους εταιρικούς στόχους. Αυτός ο διαχωρισμός πραγματοποιήθηκε κυρίως για να μπορούν να εφαρμοστούν τα 8 privacy patterns στους κατάλληλους στόχους, καθώς επίσης και για να γίνει η συσχέτιση "Επηρεάζει" μεταξύ στόχων ιδιωτικότητας και εταιρικών στόχων.

Επίσης μπορούμε να δούμε πως η οντότητα ζήτημα πηγάζει από την τετράδα Απειλή, Ευκαιρία, Αδυναμία, Δύναμη. Η συγκεκριμένη τετράδα είναι υιοθετημένη από την SWOT Analysis του Albert Humphrey. Η μεθοδολογία SWOT χρησιμοποιείται για να καταγράφονται και να αναλύονται, όπως προδίδει και το όνομα της μεθοδολογίας, οι δυνάμεις ενός συστήματος σε σχέση με τα ανταγωνιστικά του, οι αδυναμίες που έχει και τις απειλές από τις οποίες κινδυνεύει ένα πληροφοριακό σύστημα, καθώς επίσης και τις ευκαιρίες από τις οποίες μπορεί να επωφεληθεί το σύστημά μας για να αναπτυχθεί. Η Pris χρησιμοποιεί τα αποτελέσματα μίας ανάλυσης SWOT ώστε να αναγνωρίσει στόχους ιδιωτικότητας του οποίου πρέπει να φέρει εις πέρας.

Η μεθοδολογία Pris, αποτελείται από τέσσερα ξεχωριστά βήματα:

- Αναγνώριση στόχων ιδιωτικότητας
- Ανάλυση των επιπτώσεων των στόχων ασφαλείας στους εταιρικούς στόχους
- Επανασχεδίαση επηρεαζόμενων στόχων υπό το πρίσμα μοτίβων ιδιωτικότητας
- Αναγνώριση βέλτιστων μηχανισμών προς εφαρμογή μοτίβου ιδιωτικότητας επί της επηρεαζόμενης διαδικασίας

Σχόλιο [C12]: Μιλαω Ελληνικος very best και γινομαι bester and bester by the weather.

5.3 Ανάλυση βημάτων Pris

5.3.1 Αναγνώριση στόχων ιδιωτικότητας

Αρχικά αναγνωρίζουμε τους στόχους ιδιωτικότητας. Η μεθοδολογία Pris καθορίζει τους όλους τους στόχους του συστήματος ως κόμβους ενός μονής κατεύθυνσης γράφο. Οι συνδέσεις μεταξύ των στόχων λειτουργούν ως συνδέσεις μεταξύ των κόμβων του γράφου. Σε αυτό το σημείο, η μεθοδολογία Pris αποκαλύπτει δύο επιπλέον τύπους συσχετίσεων μεταξύ κόμβων. Την συσχέτιση "υποστηρίζει" και την συσχέτιση "έρχεται σε διένεξη".

Επιπλέον, αντί για γράφο, μπορούμε να έχουμε έναν δισδιάστατο πίνακα ο οποίος θα μπορεί να απεικονίζει τους στόχους και τις μεταξύ τους συσχετίσεις. Στην παρακάτω εικόνα μπορείτε να δείτε ένα τέτοιο παράδειγμα.

	G_1	$G_{1.1}$	$G_{1.2}$	$G_{1.1.1}$	$G_{1.1.2}$	$G_{1.1.3}$	$G_{1.1.3.1}$	$G_{1.1.3.2}$
G_1	0	2	2	0	0	0	0	0
$G_{1.1}$	0	0	0	2	2	2	0	0
$G_{1.2}$	0	0	0	0	0	0	0	0
$G_{1.1.1}$	0	0	0	0	0	0	0	0
$G_{1.1.2}$	0	0	0	0	0	0	0	0
$G_{1.1.3}$	0	0	3	0	0	0	2	2
$G_{1.1.3.1}$	0	0	0	0	0	0	0	0
$G_{1.1.3.2}$	0	0	0	0	0	0	0	0

ΕΙΚΟΝΑ 33 ΠΕΡΙΓΡΑΦΗ ΣΤΟΧΩΝ ΣΕ ΠΙΝΑΚΑ

Στους άξονες x,y έχουμε τους στόχους του συστήματος. Κάθε κελί αναπαριστά την συσχέτιση μεταξύ των 2 στόχων που τέμνονται στο συγκεκριμένο κελί. Η τιμή 0 χρησιμοποιείται για να αναπαραστήσει πως δεν υπάρχει συσχέτιση μεταξύ των 2 στόχων. Οι τιμές [1,4] χρησιμοποιούνται για να περιγράψουν τις συσχετίσεις μεταξύ των στόχων με τις εξής ερμηνείες. Συνολικά, οι σχέσεις καταγράφονται στον παρακάτω πίνακα.

Αριθμητική Τιμή	Ερμηνεία
0	Καμία συσχέτιση
1	Και
2	Ή
3	Υποστηρίζει
4	Έρχεται σε διένεξη

5.3.2 Ανάλυση επιπτώσεων

Το πρώτο βήμα ενός αναλυτή, όταν εισέρχεται σε αυτό το βήμα είναι να διασυνδέσει τους στόχους ιδιωτικότητας με τις διαδικασίες οι οποίες επηρεάζονται από τους στόχους. Στην συνέχεια πρέπει να αναγνωριστούν τα επονομαζόμενα μοτίβα ιδιωτικότητας (Unobservability, Undetectability κλπ.), τα οποία θα πρέπει να εφαρμοστούν πάνω στις επηρεαζόμενες διαδικασίες του συστήματος καθώς επίσης και να οδηγήσουν τον αναλυτή να επιλέξει κατάλληλους μηχανισμούς ιδιωτικότητας, οι οποίοι θα καλύπτουν επαρκώς τις απαιτήσεις ιδιωτικότητας του συστήματος.

Σε αυτό εδώ το σημείο, η Pris προτείνει την χρήση ενός μηχανισμού που ονομάζει "μεταβλητή μοτίβου διαδικασίας". Θέτουμε για κάθε διαδικασία εφτά διαφορετικές μεταβλητές οι οποίες μπορούν να πάρουν την τιμή 0 και 1. Η τιμή 1 ορίζει πως το συγκεκριμένο μοτίβο διαδικασίας θα οριστεί σε μία διαδικασία, ενώ το 0 ορίζει το αντίθετο.

5.3.3 Επανασχεδίαση επηρεαζόμενων στόχων

Η Pris για να βοηθήσει τον αναλυτή να επανασχεδιάσει ή απλώς να αναθεωρήσει τους επηρεαζόμενους στόχους, με σκοπό να βελτιώσει την ιδιωτικότητά τους, προτείνει τον εξής διαχωρισμό των μοτίβων ιδιωτικότητας σε δύο ομάδες. Τα τέσσερα πρώτα μοτίβα (Αυθεντικότητα, Εξουσιοδότηση, Αναγνώριση, Προστασία Δεδομένων) σχετίζονται με το γεγονός ότι προσπαθούμε να ενισχύσουμε την ιδιωτικότητα, αναγνωρίζοντας ξεχωριστά κάθε υποκείμενο που αλληλοεπιδρά με το σύστημα και του αναθέτουμε δικαιώματα πρόσβασης βάσει του κάθε αντικειμένου που προσπαθεί να προσπελάσει. Τα υπόλοιπα τέσσερα μοτίβα ιδιωτικότητας (Ανωνυμία, Ψευδωνυμία, Μη-συνδεσιμότητα, Μη-παρατηρησιμότητα) αποτελούν την δεύτερη ομάδα και ενισχύουν την ιδιωτικότητα του συστήματος, εστιάζοντας στην προστασία της ταυτότητας κάθε υποκειμένου του συστήματος, ή προστατεύοντας τα προσωπικά δεδομένα του εκάστοτε υποκειμένου.

Βάσει της συγκεκριμένης κατηγοριοποίησης μπορούμε να προχωρήσουμε στην επόμενη πρόταση της Pris η οποία είναι η ιεραρχία αυτών των μοτίβων ιδιωτικότητας. Η ιεραρχία των μοτίβων καθορίζει πως όσο πιο ψηλά στην ιεραρχία βρίσκεται ένα μοτίβο, τόσο πιο πολλές απαιτήσεις καλύπτει. Για παράδειγμα αν η υπάρχει απαίτηση ιδιωτικότητας για εξουσιοδότηση και έχουμε ήδη εφαρμόσει κάποιο μοτίβο αναγνώρισης, σημαίνει πως έχουμε ήδη καλύψει την απαίτηση εξουσιοδότησης. Οι 2 ιεραρχίες βάσει των 2 κατηγοριών που έχει ορίσει η Pris είναι οι εξής:

$$\text{Προστασία Δεδομένων} > \textit{Αναγνώρισης} > \textit{Εξουσιοδότησης} > \textit{Αυθεντικότητας}$$

$$\textit{Μη Παρατηρησιμότητα} > \textit{Μη Συνδεσιμότητα}$$

Τα μοτίβα ιδιωτικότητας Ψευδωνυμία και Ανωνυμία, ενώ βρίσκονται στην δεύτερη ομάδα μοτίβων, δεν εμπεριέχονται σε καμία ιεραρχία καθώς δεν σχετίζονται άμεσα με τα άλλα δύο στοιχεία της ομάδας τους όταν εφαρμόζονται πάνω σε διαδικασίες.

Η απόδοση των μοτίβων ιδιωτικότητας στις διεργασίες γίνονται με τον ορισμό ενός συνόλου μεταβλητών οι οποίες παίρνουν τις τιμές [0, 1]. Αν για παράδειγμα είχαμε μια διαδικασία με απαιτήσεις ιδιωτικότητας Αυθεντικότητα, Εξουσιοδότηση, Μη Συνδεσιμότητα και Μη Παρατηρησιμότητα, το σύνολο τιμών που θα της αναθέταμε θα ήταν:

$$(0,0,1,0,0,0,1,0)$$

Κάθε θέση αντιστοιχεί σε ένα μοτίβο ιδιωτικότητας με την εξής σειρά:

- Προστασία Δεδομένων
- Αναγνώριση
- Εξουσιοδότηση
- Αυθεντικότητα
- Ανωνυμία
- Ψευδωνυμία
- Μη Παρατηρησιμότητα
- Μη Συνδεσιμότητα

Στο παραπάνω παράδειγμα ενώ έχουμε και την απαίτηση Μη Παρατηρησιμότητας και Μη Συνδεσιμότητας, έχουμε ενεργοποιήσει μόνο μία εκ των δύο απαιτήσεων και πιο συγκεκριμένα την Μη Παρατηρησιμότητα, καθώς βάσει της ιεραρχίας που έχουμε θέσει, καλύπτει και την απαίτηση Μη

Συνδεσιμότητας. Σε περίπτωση που υπάρχει διαδικασία που πραγματοποιεί παραπάνω από ένα στόχους και κάθε στόχος έχει διαφορετικές απαιτήσεις ιδιωτικότητας, προσδίδουμε τέτοιο σύνολο τιμών έτσι ώστε να καλύπτονται οι απαιτήσεις και των δύο στόχων.

5.3.4 Αναγνώριση τεχνικών εφαρμογής απαιτήσεων ιδιωτικότητας

Εφόσον πια έχουμε ορίσει τα μοτίβα ιδιωτικότητας που πρέπει να εφαρμοστούν στις διαδικασίες του συστήματος, δεν μένει παρά να αναγνωρίσουμε ποιες τεχνικές μπορούμε να εφαρμόσουμε ώστε να καλυφθούν οι απαιτήσεις της εκάστοτε διαδικασίας. Για κάθε γνωστό και εφαρμόσιμο μηχανισμό ή τεχνική ιδιωτικότητας, έχουμε ορίσει ποιο είναι το σύνολο τιμών [0,1] που μπορεί να καλύψει. Βάσει αυτών των τιμών μπορούμε να εφαρμόσουμε αυτές τις τεχνικές. Οι τιμές του κάθε μηχανισμού περιγράφονται στον παρακάτω πίνακα.

	Administrative tools				Information tools				Anonymizer products, services and architectures										
	Identity management	Biometrics	Smart cards	Permission management	Monitoring and audit tools	Privacy policy generators	Privacy policy readers	Privacy compliance scanning	Browsing pseudonyms	Virtual Email addresses	Trusted third parties	Surrogate keys	Crowds	Onion Routing	DC-nets	Mix-nets	Hordes	GAP	Tor
Authentication	X	X	X	X	X														
Authorization	X	X	X	X	X														
Identification	X	X	X	X	X														
Data protection	X	X	X	X	X	X	X	X											
Anonymity and/or pseudonymity	X	X	X	X					X	X	X		X	X	X	X	X	X	X
Unlinkability											X	X		X	X	X	X	X	X
Unobservability			X	X	X												X	X	X

	Pseudonymizer tools		Track and evident erasers				Encryption tools		
	CRM personalization	Application data management	Spyware detection and removal	Browser cleaning tools	Activity traces eraser	Harddisk data eraser	Encrypting Email	Encrypting transactions	Encrypting documents
Authentication									
Authorization									
Identification									
Data protection									X
Anonymity and/or pseudonymity	X	X	X			X			
Unlinkability	X	X	X	X	X	X			
Unobservability			X	X	X	X	X	X	X

ΕΙΚΟΝΑ 34 ΜΗΧΑΝΙΣΜΟΙ ΙΔΙΩΤΙΚΟΤΗΤΑΣ

5.4 SecureTropos και Pris

Ουσιαστικά, αυτό που ξεχωρίζει την Pris από την SecureTropos και το εργαλείο της, το SecTro είναι ο τρόπος με τον οποίο διαχειρίζεται τις απαιτήσεις ιδιωτικότητας. Η SecureTropos αντιμετωπίζει τις απαιτήσεις ιδιωτικότητας χωρίς να λαμβάνει υπόψη κάποια ιεραρχία όπως η Pris. Αντιθέτως τις αντιμετωπίζει ως απλές απαιτήσεις ασφαλείας και συνεπώς δεν μπορεί να προτείνει κατάλληλους μηχανισμούς όπως η Pris.

Ο βέλτιστος τρόπος ενσωμάτωσης της νοοτροπίας της Pris στο εργαλείο SecTro, θα ήταν η εισαγωγή νέων συμβόλων μηχανισμών και περιορισμού ασφαλείας τα οποία θα χρησιμοποιούταν για να εκφράσουν τις απαιτήσεις ιδιωτικότητας. Κάτι τέτοιο είναι δυνατό, μιας και οι δύο μεθοδολογίες στηρίζονται σε μία ανάλυση του συστήματος βασισμένη σε διαδικασίες και στόχους, οπότε υπάρχει κοινό πλαίσιο αναφοράς. Η Pris έχει φροντίσει να προσφέρει μαθηματικές εκφράσεις οι οποίες περιγράφουν τις διάφορες διαδικασίες της, συνεπώς είναι εφικτή η προγραμματιστική επέκταση του SecTro.

Την χρονική στιγμή της συγγραφής αυτής της διπλωματικής, δεν υπάρχει επίσημη έκδοση του SecTro που να εφαρμόζει αυτή την λογική. Ανεπίσημες πηγές όμως, επιβεβαιώσανε πως επόμενη έκδοση του SecTro θα ενσωματώνει αυτή την λογική που μόλις περιγράψαμε.

Κεφάλαιο 6

SaferTec / Case Study

6.1 SaferTec

Κάθε μεθοδολογία που εξετάσαμε (EBIOS, SecureTropos, Pris) συντελούν μοναδικά, ώστε να αναπτυχθεί ένα ασφαλές και με σεβασμό προς την ιδιωτικότητα του χρήστη σύστημα. Μέχρι τώρα, αυτό που έλειπε από την συλλογή εργαλείων ενός αναλυτή κατά την διάρκεια μελέτης ενός συστήματος, ήταν μία μεθοδολογία που θα υποδείχνει την σειρά και τον τρόπο με τον οποίο θα πρέπει εφαρμοστούν αυτές οι τεχνικές ώστε να μην υπάρχουν διενέξεις μεταξύ τους και να μεγιστοποιούνται τα οφέλη της κάθε μίας.

Το συγκεκριμένο πρόβλημα έρχεται να καλύψει η μεθοδολογία SaferTec (22). Η μεθοδολογία SaferTec χρησιμοποιεί τις μεθοδολογίες που έχουμε ήδη περιγράψει και περιγράφει έξι διακριτά βήματα με τα οποία μπορούν να συνδυαστούν οι ήδη υπάρχουσες μεθοδολογίες. Ποιο συγκεκριμένα, καθορίζονται έξι βήματα μαζί με τις εισόδους που απαιτεί το κάθε βήμα, καθώς και οι έξοδοι που παράγονται. Τα έξι βήματα είναι τα εξής:

- Αναγνώριση στοιχείων συστήματος
- Αναγνώριση οργανωτικής δομής συστήματος
- Αναγνώριση περιορισμών ασφαλείας και ιδιωτικότητας
- Μοντελοποίηση απειλών και επιθέσεων
- Αναγνώριση απαιτήσεων ασφαλείας και ιδιωτικότητας
- Ανάλυση απαιτήσεων ασφαλείας και ιδιωτικότητας

6.1.1 Αναγνώριση στοιχείων συστήματος

Σε αυτό το στάδιο, ο αναλυτής χρησιμοποιεί την EBIOS για να αναγνωρίσει και να καταγράψει τα στοιχεία του συστήματος. Ως εισόδους αυτού του βήματος έχουμε τις όποιες συνεντεύξεις έχει πραγματοποιήσει ο αναλυτής με τα ενδιαφερόμενα μέρη του συστήματος, της γενικές απαιτήσεις του συστήματος αλλά και τις όποιες δηλώσεις των πολιτικών του οργανισμού οι οποίες μπορούν να επηρεάσουν την λειτουργία και την ανάπτυξη του υπό μελέτη συστήματος.

6.1.2 Αναγνώριση οργανωτικής δομής συστήματος

Στόχος αυτού του μέρους της διαδικασίας της SaferTec είναι να γίνει κατανοητό το τρέχον οργανωτικό πλαίσιο του συστήματος ώστε να ταυτοποιηθούν οντότητες όπως στόχοι, πόροι, προσφερόμενες υπηρεσίες και υποδομές που μπορεί να απαιτηθούν από το σύστημα. Τα στοιχεία τα οποία μόλις παραθέσαμε, αποτελούν τα δεδομένα εξόδου αυτής της διαδικασίας. Δεδομένα εισόδου αυτού του βήματος αποτελούν λίστες οι οποίες θα καταγράφουν τα στοιχεία του συστήματος τα οποία έχουν αναγνωρισθεί από το προηγούμενο βήμα. Επίσης τα εργαλεία τα οποία θα χρησιμοποιηθούν από τον αναλυτή είναι η Secure Tropos και η Pris.

6.1.3 Αναγνώριση περιορισμών ασφαλείας και ιδιωτικότητας

Έχοντας αναγνωρισθεί οι κύριες οντότητες του συστήματος, ο αναλυτής είναι πλέον σε θέση να αρχίσει να ασχολείται με την ασφάλεια και την ιδιωτικότητα του συστήματος. Η SaferTec εισάγει έναν νέο όρο ο οποίος δεν είχε χρησιμοποιηθεί από τις προηγούμενες τρείς μεθοδολογίες, τον όρο ευαισθησίες. Οι περιορισμοί στους οποίους θα υπόκειται ένα σύστημα είναι άρρηκτα συνδεδεμένοι, με την νοοτροπία των ενδιαφερόμενων μερών του συστήματος περί ιδιωτικότητας και ασφάλειας. Συνεπώς είναι κρίσιμης σημασίας να αναγνωρισθούν οι θέσεις ή αλλιώς ευαισθησίες που έχουν τα

ενδιαφερόμενα μέρη. Συνεπώς ως δεδομένα εισόδου αυτού του βήματος θεωρούνται οι ευαισθησίες των ενδιαφερόμενων μερών, οι τυχόν νομικές και κανονιστικές υποχρεώσεις στις οποίες υπάγεται το σύστημα, η πολιτική ασφαλείας του οργανισμού και οι στόχοι του οργανισμού. Από αυτά τα δεδομένα και με το πέρας αυτού του βήματος, ο αναλυτής θα πρέπει να έχει στην διάθεσή του μία λίστα στην οποία θα καταγράφονται οι ευαισθησίες των ενδιαφερόμενων μερών, οι περιορισμοί ιδιωτικότητας και ασφάλειας του συστήματος και οι σχέσεις μεταξύ των στόχων του συστήματος και των περιορισμών ιδιωτικότητας και ασφάλειας. Τα εργαλεία που χρησιμοποιούνται για την τέλεση αυτού του βήματος είναι η EBIOS, η SecureTropos και η Pris.

6.1.4 Μοντελοποίηση απειλών και επιθέσεων

Κατά την διάρκεια αυτού του βήματος αναγνωρίζονται απειλές και τρόποι επίθεσης οι οποίοι μπορούν να εκθέσουν το σύστημα σε κίνδυνο. Αν δεν πραγματοποιηθεί εξονυχιστική μελέτη περί απειλών και επιθέσεων, ο αναλυτής του συστήματος δεν θα μπορεί να είναι σε θέση να εξάγει σωστές απαιτήσεις ιδιωτικότητας και ασφάλειας σε παρακάτω βήμα της διαδικασίας. Για να γίνει σωστή ανάλυση απειλών και τρόπων επιθέσεων, ο αναλυτής χρειάζεται τα δεδομένα που εξήχθησαν από το προηγούμενο βήμα της μεθοδολογίας με σκοπό να παράγει λίστες απειλών και τρόπων επιθέσεων.

6.1.5 Αναγνώριση απαιτήσεων ασφαλείας και ιδιωτικότητας

Αναγνωρίζοντας τις απειλές και τους τρόπους επίθεσης ενός συστήματος, ο αναλυτής είναι πλέον σε θέση να ορίσει τις απαιτήσεις ασφαλείας και ιδιωτικότητας με σκοπό να ελαττώσει το ρίσκο στο οποίο υπόκειται το πληροφοριακό σύστημα. Αυτό το βήμα αποτελεί ένα εξίσου κρίσιμο βήμα στην διαδικασία της SaferTec, καθώς η σωστή αναγνώριση απαιτήσεων θα βοηθήσει στην ελάττωση των επιπέδων ρίσκου του πληροφοριακού συστήματος, με το πέρας και του επόμενου βήματος της διαδικασίας. Δεδομένα εισόδου του συγκεκριμένου βήματος αποτελούν τα δεδομένα εξόδου του προηγούμενου βήματος. Τα δεδομένα εξόδου είναι δύο λίστες οι οποίες συσχετίζουν στοιχεία του πληροφοριακού συστήματος με απαιτήσεις ιδιωτικότητας και ασφάλειας.

6.1.6 Ανάλυση απαιτήσεων ασφαλείας και ιδιωτικότητας

Στο τελευταίο βήμα της μεθοδολογίας SaferTec, χρησιμοποιούνται όλα τα δεδομένα που έχουν συλλεχθεί από τα προηγούμενα βήματα και αναλύονται ώστε να αναγνωρισθούν τυχόν διενέξεις μεταξύ των περιορισμών ασφάλειας και ιδιωτικότητας. Επίσης σε αυτό το στάδιο αναγνωρίζονται από τον αναλυτή τεχνικές και μηχανισμοί οι οποίοι μπορούν να εφαρμοστούν για να καλυφθούν οι αδυναμίες του συστήματος και να μειωθούν τα επίπεδα απειλής σε αποδεκτά από τα ενδιαφερόμενα μέρη, επίπεδα.

6.2 Case Study

Προς καλύτερη κατανόηση της SaferTec από τον αναγνώστη, το υπόλοιπο της διπλωματικής αυτής εργασίας, θα αφιερωθεί στην εξέταση ενός συστήματος ανταλλαγής πληροφοριών μεταξύ οχημάτων και στο πως θα εφαρμοζόταν τα βήματά της πάνω στο σύστημα. Πιο συγκεκριμένα, το συγκεκριμένο σύστημα αποτελείται από τρία επιμέρους συστήματα:

- ITS-S
- R-ITS-S (RSU)
- C-ITS-S

Το σύστημα ITS-S (Intelligent Transportation System Station) αναφέρεται στο πληροφοριακό σύστημα του εκάστοτε οχήματος. Το συγκεκριμένο σύστημα περιέχει στοιχεία που επιτρέπουν την επικοινωνία του συστήματος με εξωτερικά περιβάλλοντα, δεδομένα του οχήματος και την απαραίτητη επεξεργαστική ισχύ προς επεξεργασία των δεδομένων που προέρχονται από το εξωτερικό περιβάλλον

μέσω των αισθητήριων συστημάτων του οχήματος. Παραδείγματα δεδομένων μπορούν να αποτελούν, η ταχύτητα του οχήματος, η κατεύθυνση ή η θερμοκρασία του κινητήρα. Επίσης το ITS-S περιέχει κατάλληλους μηχανισμούς με τους οποίους καθίσταται δυνατή η επικοινωνία με τα R-ITS-S και C-ITS-S.

Το R-ITS-S (Roadside Intelligent Transportation System Station) ή αλλιώς RSU (Road Side Unit), είναι συσκευές οι οποίες όπως δηλώνει και το όνομά τους βρίσκονται δίπλα στους δρόμους. Τα στοιχεία που αποτελούν αυτό το σύστημα είναι πανομοιότυπα με το σύστημα που περιγράψαμε στην προηγούμενη παράγραφο. Οι υποχρεώσεις του συστήματος είναι και αυτές παρόμοιες, δηλαδή η συλλογή, επεξεργασία και αναμετάδοση πληροφορίας σε εξουσιοδοτημένες οντότητες του γενικότερου συστήματος. Η φύση των δεδομένων που συλλέγονται διαφέρουν από αυτή του προηγούμενου συστήματος, αλλά όχι σε μεγάλο βαθμό. Αυτό το σύστημα μπορεί να συλλέγει πληροφορίες όπως θερμοκρασία ατμόσφαιρας, ρυθμό διερχόμενων οχημάτων, ταχύτητα αέρα, επίπεδα υγρασίας κ.α.

Τελικό σύστημα του γενικότερου συστήματος, αποτελεί το C-ITS-S (Central Intelligent Transportation System Station). Στόχος αυτού του συστήματος είναι να συλλέγει τα δεδομένα των δύο προηγούμενων συστημάτων, να τα συσχετίζει και να εξάγει περισσότερη πληροφορία από τα δεδομένα. Συνεπώς μέσω αυτών των δεδομένων, οι χρήστες του συστήματος θα μπορούν να έχουν πρόσβαση σε μία περισσότερο ολοκληρωμένη εικόνα της κατάστασης που επικρατεί σε διάφορα τμήματα του οδικού δικτύου. Επίσης θα καθίσταται δυνατή η αποστολή γενικευμένων προειδοποιητικών μηνυμάτων στις κατάλληλες ομάδες οχημάτων σε περίπτωση που αυτό χρειαστεί.

6.3 Ανάλυση C-ITS-S

Στα πλαίσια αυτής της διπλωματικής εργασίας, ζητήθηκε από τον συγγραφέα να εφαρμοστούν ορισμένα βήματα της SaferTec στο σύστημα C-ITS-S. Τα υπόλοιπα βήματα της μεθοδολογίας δεν είναι δυνατόν να πραγματοποιηθούν όπως θα έπρεπε, καθώς απαιτούνται δεδομένα (συνεντεύξεις, γενικότερο πλαίσιο πληροφοριακού συστήματος) τα οποία ο συγγραφέας, την χρονική περίοδο της συγγραφής αυτής της διπλωματικής εργασίας, δεν έχει στην κατοχή του.

6.3.1 Αναγνώριση στοιχείων C-ITS-S

Αρχικά, όπως ορίζει και η SaferTec, θα πρέπει να αναγνωρίσουμε τα διάφορα στοιχεία του πληροφοριακού συστήματος. Το μόνο που γνωρίζουμε για το συγκεκριμένο σύστημα, είναι πως πρόκειται για εφαρμογή η οποία φιλοξενείται σε νεφοϋπολογιστική δομή. Συνεπώς θα χρησιμοποιήσουμε ένα γενικό μοντέλο νεφοϋπολογιστικής δομής για να περιγράψουμε το σύστημα C-ITS-S.

Η γενική δομή ενός τέτοιου συστήματος αποτελείται από πέντε διαφορετικά στοιχεία:

- Επεξεργαστική υποδομή
- Αποθηκευτική υποδομή
- Σύστημα εικονοποίησης
- Διεπαφές συστήματος
- Εφαρμογή

Η επεξεργαστική υποδομή, αναφέρεται στο hardware το οποίο είναι υπεύθυνο να προσφέρει υπηρεσίες επεξεργασίας δεδομένων. Σε αυτό το σύστημα συμπεριλαμβάνονται στοιχεία όπως τα φυσικά μηχανήματα (επεξεργαστές, μνήμες RAM) αλλά και ολόκληρο το κτηριακό οικοδόμημα το οποίο φιλοξενεί τις υποδομές του συστήματος

Η αποθηκευτική υποδομή μοιάζει με την επεξεργαστική υποδομή. Η διαφορά της είναι πως αναφέρεται στην αποθήκευση και ανάκτηση των δεδομένων καθώς και με τα ίδια τα δεδομένα που διαχειρίζεται. Επίσης έχουμε της φυσικές υποδομές που προσφέρουν αυτές τις δυνατότητες στην

αποθηκευτική υποδομή, όπως τα φυσικά αποθηκευτικά μέσα, το λογισμικό βάσης δεδομένων που διαχειρίζεται τα δεδομένα, καθώς επίσης και τις λοιπές απαιτούμενες φυσικές υποδομές.

Το σύστημα εικονοποίησης είναι αυτό που ξεχωρίζει την νεφοϋπολογιστική υποδομή με τα υπόλοιπα συστήματα φιλοξενίας εφαρμογών. Το σύστημα εικονοποίησης φροντίζει ώστε οι υπάρχοντες φυσικοί πόροι που διαθέτουμε, να χωρίζονται σε διακριτά συστήματα χωρίς αυτά να υπάρχουν στην πραγματικότητα. Αυτό σημαίνει πως μπορούμε με ένα σύστημα εικονοποίησης να μετατρέψουμε ένα φυσικό μηχάνημα σε περισσότερα αλλά σαφέστατα πιο αδύναμα μηχανήματα. Τα οφέλη αυτής της πρακτικής εμφανίζονται όταν χρειαζόμαστε να φιλοξενήσουμε εφαρμογές σε υποδομές οι οποίες είναι μακράν επαρκέστερες των αναγκών της εφαρμογής. Η μέθοδος προσέγγισης με εικονικές μηχανές, βοηθά στο να αξιοποιούνται σε μεγαλύτερο βαθμό οι πόροι ενός φυσικού συστήματος αλλά γίνεται και ευκολότερη η διαχείριση πολλαπλών μηχανημάτων, εφόσον είναι εικονικά.

Οι διεπαφές του συστήματος είναι όλα τα στοιχεία τα οποία βοηθούν το σύστημα να αλληλοεπιδρά με τον έξω κόσμο. Επίσης υπάρχουν διεπαφές στο σύστημα οι οποίες είναι εσωτερικές και είναι υπεύθυνες για την πραγματοποίηση επικοινωνίας μεταξύ των υποδομών του συστήματος. Στοιχεία υποδομών μπορεί να αποτελεί το εσωτερικό IP δίκτυο, η διασύνδεση με το Διαδίκτυο ή μία σύνδεση VPN.

Τέλος, έχουμε το στοιχείο της εφαρμογής. Όλες αυτές οι τεχνολογίες οι οποίες συγκεντρώθηκαν μαζί για να αποτελέσουν ένα νεφοϋπολογιστικό σύστημα δεν θα είχαν καμία αξία αν δεν φιλοξενούσαν μία εφαρμογή. Με τον όρο εφαρμογή, αναφερόμαστε στο λογισμικό το οποίο αξιοποιούν εξωτερικοί χρήστες του συστήματος το οποίο τους προσφέρει κάποια υπηρεσία. Υπάρχουν νεφοϋπολογιστικές δομές οι οποίες μπορούν να φιλοξενούν πολλαπλές εφαρμογές. Για το παράδειγμά μας όμως, θα θεωρήσουμε πως η δομή μας φιλοξενεί μία εφαρμογή.

6.3.2 Αναγνώριση οργανωτικής δομής του συστήματος

Το συγκεκριμένο βήμα της διαδικασίας δεν είναι δυνατόν να πραγματοποιηθεί πλήρως, λόγω ελλιπής ύπαρξης δεδομένων. Να υπενθυμίσουμε στον αναγνώστη πως το συγκεκριμένο βήμα της SaferTec παράγει τους στόχους του συστήματος, καταγράφει τους πόρους του και σκιαγραφεί την οργανωτική δομή του. Όλα αυτά τα δεδομένα παράγονται με βοήθεια των αποτελεσμάτων μίας μεθοδολογίας διαχείρισης κινδύνου, όπως η μεθοδολογία EBIOS την οποία αναλύσαμε σε προηγούμενο κεφάλαιο. Για τους λόγους που μόλις εξηγήσαμε, θα προχωρήσουμε στο επόμενο βήμα της SaferTec δίνοντας παραδείγματα των αποτελεσμάτων που θα παρήγαγε η μεθοδολογία αν υπήρχαν πλήρη δεδομένα.

6.3.3 Αναγνώριση περιορισμών ιδιωτικότητας και ασφάλειας

Άλλο ένα βήμα για το οποίο χρειαζόμαστε πληροφορίες που δεν έχουμε στην διάθεσή μας. Στο συγκεκριμένο βήμα χρησιμοποιούμε πληροφορίες που έχουμε συλλέξει κατά την διάρκεια των συνεντεύξεων που προβλέπει η διαδικασία διαχείρισης κινδύνου. Όπως αναφέραμε και προηγουμένως, το συγκεκριμένο βήμα απαιτεί να γνωρίζουμε τις ευαισθησίες των ενδιαφερόμενων μερών για να αναγνωρίσουμε τους περιορισμούς στους οποίους θα υπόκειται το σύστημα. Εφόσον όμως δεν έχουμε στην διάθεσή μας αντίστοιχα δεδομένα, θα προχωρήσουμε στο επόμενο βήμα της SaferTec.

6.3.4 Μοντελοποίηση απειλών και επιθέσεων

Η νεφοϋπολογιστική φύση του συστήματος C-ITS-S, είναι αυτή που μας επιτρέπει να προχωρήσουμε κανονικά σε αυτό το βήμα της SaferTec. Ανεξαρτήτως της εφαρμογής που φιλοξενείται

στις υποδομές μίας νεφοϋπολογιστικής δομής, υπάρχουν απειλές, αδυναμίες και επιθέσεις οι οποίες θα αναγνωρίζονται ανεξαρτήτως εφαρμογής. Σε αυτή την ενότητα θα συσχετίσουμε τα διάφορα στοιχεία της νεφοϋπολογιστικής δομής που περιγράψαμε, με επιθέσεις και απειλές. Αρχικά θα πραγματοποιήσουμε έναν πίνακα ο οποίος θα καταγράφει παραδείγματα απειλών όπως αυτές σχετίζονται με τα στοιχεία του συστήματος.

Στοιχείο	Απειλή	Επηρεαζόμενη Απαίτηση Ασφάλειας	Σχόλιο	Προτεινόμενο Αντίμετρο
Επεξεργαστική Υποδομή	Απώλεια ελέγχου υποδομών	Εμπιστευτικότητα Ακεραιότητα Εξουσιοδότηση Υπαγωγή στον Νομο	Χαρακτηριστικά του υπολογιστικού νέφους όπως η δυναμική ιδιοκτησία (dynamic ownership), συλλογικά/διαμοιραζόμενα αποθηκευτικά μέσα (collaborative storage), συλλογές εξυπηρετών (server pool), επιτόπια αποθήκευση (data locality) πλησίον του σημείου επεξεργασίας κ.α. μειώνουν τον έλεγχο που έχει ο πελάτης πάνω στην υποδομή του.	Δυνατότητα καλύτερου ελέγχου από τον χρήστη της υπηρεσίας που χρησιμοποιεί όπως on demand installation, reboot, reconfigure σε IaaS υποδομές
	Φωτιά	Ακεραιότητα Υπαγωγή στον Νόμο Διαθεσιμότητα	Κίνδυνος ύπαρξης πυρκαγιάς η οποία θα επηρεάσει την λειτουργία του συστήματος	Επαρκή μέτρα πυρόσβεσης Ύπαρξη backup
	Μη αξιόπιστη επεξεργασία δεδομένων στο cloud	Ακεραιότητα Εμπιστοσύνη	Πρόβλημα επιβεβαίωσης της ορθότητας των υπολογισμών του υπολογιστικού νέφους.	Σύγκριση των αποτελεσμάτων της επεξεργασίας στο cloud διαφορετικών παρόχων από τον πελάτη ώστε να διαλέξει αυτή που θεωρεί πιο αξιόπιστη πριν την ενοικίαση κάποιας υπηρεσίας, πολλοί πάροχοι παρέχουν δωρεάν χρήση υπηρεσιών για λόγους

				αξιολόγησης, trial usage, Amazon EC2, Microsoft Azure
	Διακοπή εύρυθμης λειτουργίας υπολογιστικού νέφους	Διαθεσιμότητα	Μπορεί να οφείλεται σε μικρολάθη υπολογισμών (single bit error), υπερφόρτωση υπηρεσίας, προγραμματιστικά σφάλματα, προβλήματα σε πρωτόκολλα και στο δίκτυο	Ενδελεχή δοκιμή νέου προϊόντος πριν ενταχθεί σε production περιβάλλον, χρήση redundant συστημάτων επεξεργαστικής και δικτυακής υποδομής, load balancin
	Υπερκατανάλωση πόρων από άλλους πελάτες της cloud υπηρεσίας	Διαθεσιμότητα	Ένας κακόβουλος πλην νόμιμος πελάτης ενός υπολογιστικού νέφους μπορεί να δημιουργεί συνεχώς αιτήματα προς επεξεργασία για την υποδομή, προκειμένου να καταναλώνει όλους τους διαθέσιμους πόρους και τελικά να επιτύχει την άρνηση παροχής πόρων προς άλλους πελάτες της υποδομής. Το πρόβλημα αυτό μετριάζεται από το κόστος που θα πρέπει να καταβάλλει ο επιτιθέμενος και από τις δυνατότητες τις υποδομής για καταμερισμό του φόρτου.	Εγκατάσταση monitoring συστημάτων για τον άμεσο εντοπισμό κατάχρησης υπολογιστικών πόρων και περιορισμός ή τερματισμός της υπηρεσίας στον συγκεκριμένο πελάτη, Nagios Monitoring System
Αποθηκευτική υποδομή	Data Storage Location	Εμπιστοσύνη	Ο χρήστης δεν γνωρίζει που βρίσκονται τα δεδομένα του ανά πάσα χρονική στιγμή, σε πιο server, σε ποια χώρα, μπορεί να μην επιθυμεί να βρίσκονται σε κάποια συγκεκριμένη χώρα.	Ενημέρωση του χρήστη κατά την σύναψη της συμφωνίας και της αποδοχής του EULA ότι τα δεδομένα θα βρίσκονται σε αυτή την συγκεκριμένη χώρα και μπορεί
	Διασκορπισμός σε πολλές περιοχές	Υπαγωγή στον Νομο	Δεδομένα διαμοιράζονται για redundancy σε διαφορετικές και περιοχές και σε μπορεί και σε διαφορετικά κράτη, αυτό μπορεί να προκαλέσει	

			νομικά προβλήματα ή προβλήματα συμμόρφωσης με πρότυπα καθώς τα δεδομένα διασχίζουν σύνορα	να ελεγχθούν για αξιόποινες πράξεις από τα όργανα τάξης αυτής της χώρας, συμβουλευτική από εξειδικευμένους νομικούς για το νομικό πλαίσιο διατήρησης πληροφοριών ανά χώρα
	Αποκάλυψη μοτίβων προσπέλασης του χρήστη (Access Patterns) στον αποθηκευτικό χώρο στο cloud	Εμπιστευτικότητα	Αν και τα αρχεία του χρήστη στον απομακρυσμένο server cloud μπορεί να είναι κρυπτογραφημένα, τα μοτίβα προσπέλασης σε αυτά ενέχουν τον κίνδυνο αποκάλυψης πληροφορίας από κακόβουλο διαχειριστή της cloud υπηρεσίας	Χρήση σύγχρονων τεχνολογιών απόκρυψης μοτίβων προσπέλασης στα δεδομένα, ORAM τεχνολογίες, Oblivistor, Blind Sheer
	Δυσχέρεια επαληθευσιμότητας και ακεραιότητας δεδομένων	Ακεραιότητα	Πρόβλημα επιβεβαίωσης ορθής αποθήκευσης και διαχείρισης δεδομένων από το υπολογιστικό νέφος.	Χρήση λίστας δικαιωμάτων πρόσβασης, και role based access στους πόρους.
Εικονοποίηση	Κλοπή εικόνων (images) και έγχυση κώδικα σε πρότυπα εικόνων και στιγμιότυπα	Εμπιστευτικότητα Ακεραιότητα		Υπογραφή ακεραιότητας της εικόνας
	Κρυπτογραφικός φόρτος προστασίας εικόνων	Ασφάλεια συστήματος Προστασία πόρων από κατάχρηση	Λόγω του μεγάλου μεγέθους και του πλήθους τους, η προστασία των εικόνων με κρυπτογραφικές μεθόδους κατά την αδράνεια, αποθήκευση, μετάδοση και εν γένει επεξεργασία τους είναι μια δαπανηρή σε πόρους διαδικασία. Η μη προστασία των εικόνων, όμως, αυξάνει την ανασφάλεια του συστήματος.	Υπογραφή ακεραιότητας εικόνας

	Single point of failure, μη έμπιστα μέρη διαχειριστή εικονικών μηχανών (hypervisor, hypervisor rootkits)	Ασφάλεια συστήματος		Εφεδρικοί hypervisors
	Μη δημοσιοποιημένες (zero-day) / νέες ευπάθειες του διαχειριστή των εικονικών μηχανών (hypervisor) οι οποίες δεν έχουν ληφθεί υπόψη κατά την επιλογή των μέτρων ασφάλεια	Εμπιστευτικότητα Ακεραιότητα Διαθεσιμότητα Ασφάλεια συστήματος		Μηχανισμός ανίχνευσης κακόβουλων ενεργειών, βάσει συμπεριφοράς
Διεπαφές	Ευάλωτα πρωτόκολλα επικοινωνίας, δικτυακές επιθέσεις συνοικούντων, κλοπή συνόδου, λανθασμένη υλοποίηση του πρωτοκόλλου HTTPS, μείξη ροών HTTP και HTTPS, λανθασμένη χρήση τυχαιότητας για την παραγωγή/διαχείριση κρυπτογραφικών κλειδιών, κλοπή και επαναχρησιμοποίηση cookies, κακόβουλη τροποποίηση cookies, επιθέσεις πλαστοπροσωπίας, επιθέσεις κατά του πρωτοκόλλου TLS	Εμπιστευτικότητα Ακεραιότητα Διαθεσιμότητα Εξουσιοδότηση Ιδιωτικότητα		Απομόνωση δικτύων
	Virtual Private Server (VPS) bots, άμεσες/στοχευμένες και έμμεσες/παράπλευ	Διαθεσιμότητα Προστασία πόρων από κατάχρηση	Η υποδομή υπολογιστικού νέφους ενδέχεται να αποπειραθεί να αντιδράσει σε επιθέσεις άρνησης εξυπηρέτησης ή πλημμύρας	Διαχωρισμός στατικών και δυναμικών οντοτήτων του δικτύου

	ρες επιθέσεις άρνησης εξυπηρέτησης (DoS), καταστάσεις ανταγωνισμού, επιθέσεις πλημμύρας UDP uplink, επιθέσεις εξάντλησης πόρων, επιθέσεις XML πλημμύρας, επιθέσεις ανάκλασης και ενίσχυσης DNS		με την μετεγκατάσταση των φιλοξενούμενων υπηρεσιών σε άλλα σημεία της υποδομής, όμως, εάν πρόκειται για συντονισμένη επίθεση αυτό μπορεί να οδηγήσει στην εξάπλωση της επίθεσης σε όλη την υποδομή. Επίσης εάν η επίθεση προέρχεται από την ίδια την υποδομή του υπολογιστικού νέφους (π.χ. από κάποιων κακόβολο εσωτερικό χρήστη ή πελάτη) η υποδομή κινδυνεύει να μπει σε μια κατάσταση ανταγωνισμού, όπου η παροχή περισσότερων πόρων για την εξυπηρέτηση της επίθεσης αντικατοπτρίζεται από μια ανάλογη μεγέθυνση της επίθεσης έως ότου εξαντληθούν όλοι οι πόροι του συστήματος.	
	Ανεπαρκείς δυνατότητες καταγραφής και διαχειριστικής παρακολούθησης	Έλεγχος Προστασία πόρων από κατάχρηση	Ο όγκος καταγραφών μπορεί να είναι δυσανάλογα μεγάλος προς το μέγεθος των εν δυνάμει επιτηρητών	
	Ευπάθειες διαδικασίας ανάκτησης / επαναφοράς διαπιστευτηρίων	Εξουσιοδότηση Υπαγωγή στον Νόμο Εξουσιοδότηση Υπαγωγή στον Νομο Αυθεντικοποίηση Ασφάλεια Συστήματος Προστασία πόρων από Κατάχρηση	Ανασφαλείς διαδικασίες ανάκτησης ή επαναφοράς διαπιστευτηρίων (π.χ. συνθηματικών) μπορεί να επιτρέψουν σε επιτιθέμενους να αποκτήσουν πρόσβαση στο σύστημα.	Τοποθέτηση κρυπτογραφημένων διαπιστευτηρίων σε τοποθεσίες με αυξημένη προστασία και όσο γίνεται απομονωμένες από άλλες υπηρεσίες.
	Ανεπαρκές επίπεδο αυθεντικοποίησης	Αυθεντικοποίηση Εξουσιοδότηση	Οι μηχανισμοί Single Sign-On (SSO) μπορεί να βοηθήσουν στη μείωση της πολυπλοκότητας που ενέχει η	Σωστή υλοποίηση του SSO πρωτοκόλλου,

			χρήση πολύ-επίπεδων (πολλών παραγόντων) μηχανισμών εισόδου για πολλές υπηρεσίες. Ωστόσο, η χρήση τους δε πρέπει να θεωρείται πανάκεια , καθώς στο παρελθόν έχουν βρεθεί πολλές ευπάθειές, που οδήγησαν σε επιθέσεις πλαστοπροσωπίας ή παράκαμψης της αυθεντικοποίησης/εξουσιοδότησης.	και συνεχής επίβλεψη του για νέες εκδόσεις και επιθέσεις που μπορούν να προκύψουν.
Εφαρμογή	Έκθεση στο Διαδίκτυο των διεπαφών διαχείρισης, ευπάθειες κονσόλας διαχείρισης επιμελητή εικονικών μηχανών VMM (Virtual Machine Manager)	Εξουσιοδότηση Ορθή τεχνοδιαμόρφωση	Κακόβουλοι επιτιθέμενοι μπορούν να εκμεταλλευτούν ευπάθειες της διεπαφής διαχείρισης ώστε να αποκτήσουν πρόσβαση σε δεδομένα και πόρους ή να τροποποιήσουν την τεχνοδιαμόρφωση του συστήματος.	Web Application Firewalls, Role based Access
	Κενά ασφάλειας εφαρμογής (application loopholes), κεκαλυμμένη έγχυση κώδικα (masked code injection)	Εξουσιοδότηση Ακεραιότητα	Κακόβουλοι επιτιθέμενοι μπορούν να εκμεταλλευτούν ευπάθειες της διεπαφής διαχείρισης ώστε να αποκτήσουν πρόσβαση σε δεδομένα και πόρους ή να τροποποιήσουν την τεχνοδιαμόρφωση του συστήματος.	Code review από έμπειρο και εξειδικευμένο προσωπικό, vulnerability assessments, penetration testings
	Ανεπαρκής παραμετροποίηση, μη εξουσιοδοτημένη πρόσβαση	Εξουσιοδότηση Ορθή τεχνοδιαμόρφωση	Η κακή παραμετροποίηση της διεπαφής χρήστη μπορεί να δώσει ευκολά πρόσβαση σε μη εξουσιοδοτημένα άτομα στην κονσόλα διαχείρισης εικονικών μηχανών του διαχειριστή της υπηρεσίας καθώς και στην κονσόλα διαχείρισης του λογαριασμού και των υπηρεσιών του πελάτη	Vulnerability assessment, penetration testing
	Ανασφαλείς κλήσεις συστήματος, ελαττωματικός	Διαθεσιμότητα Λειτουργικός Ελεγχος	Δύσκολη η διαχείριση της μνήμης και ο on demand τερματισμός νημάτων διεργασιών σε υποδομές	Χρήση σύγχρονων τεχνολογιών διαχωρισμού

	περιορισμός μνήμης (process memory isolation), τερματισμός υπολογιστικών νημάτων		PaaS (.NET, Java EE) από τους παρόχους υπηρεσιών cloud σε περιπτώσεις κατάχρησης υπολογιστικών πόρων	και απομόνωσης διεργασιών, Java MVM (Multitasking-Virtual-Machine), Sandboxing

Έχοντας μοντελοποιήσει τις απειλές του συστήματος, μπορούμε να μοντελοποιήσουμε και τις επιθέσεις οι οποίες μπορούν να πραγματοποιήσουν τις απειλές. Στην συνέχεια θα καταγράψουμε ενδεικτικές επιθέσεις για κάθε απειλή την οποία αναφέραμε στον προηγούμενο πίνακα.

Απειλή	Επίθεση
Απώλεια ελέγχου υποδομών	Denial of Service Message Modification Malware Injection Eavesdropping
Φωτιά	Physical Attack Denial of Service
Μη αξιόπιστη επεξεργασία δεδομένων στο cloud	Denial of Service
Διακοπή εύρυθμης λειτουργίας υπολογιστικού νέφους	Denial of Service
Υπερκατανάλωση πόρων από άλλους πελάτες της cloud υπηρεσίας	Denial of Service Co-Residence Side Channel
Data Storage Location	Denial of Service (Ως παράγωγο της έκχυσης οικονομικών πόρων σε δικαστικές υποθέσεις)
Διασκορπισμός σε πολλές περιοχές	Denial of Service (Ως παράγωγο της έκχυσης οικονομικών πόρων σε δικαστικές υποθέσεις)
Αποκάλυψη μοτίβων προσπέλασης του χρήστη (Access Patterns) στον αποθηκευτικό χώρο στο cloud	Side Channel Attack Eavesdropping
Δυσχέρεια επαληθευσιμότητας και ακεραιότητας δεδομένων	Message Modification Malformed Frame Injection
Κλοπή εικόνων (images) και έγχυση κώδικα σε πρότυπα εικόνων και στιγμιότυπα	Malicious Code Injection Malware Injection
Κρυπτογραφικός φόρτος προστασίας εικόνων	Denial of Service
Single point of failure, μη έμπιστα μέρη διαχειριστή εικονικών μηχανών (hypervisor, hypervisor rootkits)	Denial of Service
Μη δημοσιοποιημένες (zero-day) / νέες ευπάθειες του διαχειριστή των εικονικών μηχανών (hypervisor) οι οποίες δεν έχουν ληφθεί υπόψη κατά την επιλογή των μέτρων ασφάλεια	Malware Injection Message Modification Replay Attack Malicious Code Injection Downdgrade Attack

Σχόλιο [C13]: Πως να το γραψω αυτό?

Σχόλιο [C14]: Πως να το γραψω αυτό?

	Eavesdropping
Ευάλωτα πρωτόκολλα επικοινωνίας, δικτυακές επιθέσεις συνοικούντων, κλοπή συνόδου, λανθασμένη υλοποίηση του πρωτοκόλλου HTTPS, μείξη ροών HTTP και HTTPS, λανθασμένη χρήση τυχαιότητας για την παραγωγή/διαχείριση κρυπτογραφικών κλειδιών, κλοπή και επαναχρησιμοποίηση cookies, κακόβουλη τροποποίηση cookies, επιθέσεις πλαστοπροσωπίας, επιθέσεις κατά του πρωτοκόλλου TLS	Eavesdropping Man in the middle
Virtual Private Server (VPS) bots, άμεσες/στοχευμένες και έμμεσες/παράπλευρες επιθέσεις άρνησης εξυπηρέτησης (DoS), καταστάσεις ανταγωνισμού, επιθέσεις πλημμύρας UDP uplink, επιθέσεις εξάντλησης πόρων, επιθέσεις XML πλημμύρας, επιθέσεις ανάκλασης και ενίσχυσης DNS	Distributed Denial of Service
Ανεπαρκείς δυνατότητες καταγραφής και διαχειριστικής παρακολούθησης	Man in the Middle Masquerading Routing Attack Replay Attack
Ευπάθειες διαδικασίας ανάκτησης / επαναφοράς διαπιστευτηρίων	Masquerading
Ανεπαρκές επίπεδο αυθεντικοποίησης	Masquerading
Έκθεση στο Διαδίκτυο των διεπαφών διαχείρισης, ευπάθειες κονσόλας διαχείρισης επιμελητή εικονικών μηχανών VMM (Virtual Machine Manager)	Brute-force attack
Κενά ασφάλειας εφαρμογής (application loopholes), κεκαλυμμένη έγχυση κώδικα (masked code injection)	Malicious Code Injection Malware Injection
Ανεπαρκής παραμετροποίηση, μη εξουσιοδοτημένη πρόσβαση	Masquerading Malicious Code Injection Malware Injection
Ανασφαλείς κλήσεις συστήματος, ελαττωματικός περιορισμός μνήμης (process memory isolation), τερματισμός υπολογιστικών νημάτων	Malware Injection Malicious Code Injection

Οι παραπάνω λίστες είναι ενδεικτικές και συνεπώς σε καμία περίπτωση εξαντλητικές και πλήρεις. Σκοπός τους είναι να μυήσουν τον αναγνώστη στο συγκεκριμένο βήμα της SaferTec, καθώς αποτελούν παράδειγμα το οποίο είναι δυνατόν να πραγματοποιηθεί έστω και ως παράδειγμα, δεδομένου των δεδομένων που έχει στην κατοχή του ο συγγραφεύς. Τα δύο βήματα της SaferTec δεν είναι δυνατόν να πραγματοποιηθούν λόγω έλλειψης δεδομένων σχετικά με το γενικότερο πλαίσιο και περιβάλλον του οργανισμού.

Κεφάλαιο 7

Επίλογος

7.1 Συμπεράσματα

Από την απαρχή της πληροφορικής και γενικότερα των πληροφοριακών συστημάτων έχει περάσει αρκετός καιρός, ο οποίος έχει συντελέσει σημαντικά στην ωρίμανση του πεδίου της πληροφορικής. Κάπου στην πορεία γεννήθηκε και το πεδίο της κυβερνοασφάλειας, κάτι το οποίο δεν είναι πλήρως αληθές, αν αναλογιστούμε πως το πρώτο κρυπτογράφημα χρονολογείται από το 1900 π.Χ. (23). Χάρη στην ανάπτυξη αυτών των δύο πεδίων γεννήθηκε η ανάγκη σχεδίασης συστημάτων τα οποία θα είναι ασφαλή και ταυτοχρόνως θα σέβονται την ιδιωτικότητα των χρηστών του.

Η πρώτη θεωρία περί γενικών συστημάτων καταγράφτηκε το 1968 από τον Bertalanffy όπως είδαμε και έχει επεκταθεί αρκετά ώστε να περιέχει από θεωρίες ψυχολογίας και βιολογικά συστήματα, μέχρι και συστήματα πληροφορικής, τα οποία το καθένα ξεχωριστά μπορεί να προσδίδει και κάτι διαφορετικό στην γενική θεωρία συστημάτων χωρίς όμως να προσβάλλει τον πυρήνα της θεωρίας του Bertalanffy.

Η μηχανική απαιτήσεων ήρθε να πάει το ζεύγος πληροφορικής και θεωρίας συστημάτων ένα βήμα παρακάτω, θέτοντας ένα πλαίσιο και καθ' επέκταση τις διαδικασίες που θα πρέπει να ακολουθούνται κατά την ανάπτυξη ενός πληροφοριακού συστήματος. Το παράδοξο της όλης ιστορίας είναι πως οι απαρχές της μηχανικής απαιτήσεων αποδίδονται στο (24) το οποίο χρονολογείται το 1962. Όπως και να έχει, χάρη στον συνδυασμό αυτών των δύο πεδίων και της εξέλιξης αυτών, έχουμε καταφέρει να αναπτύξουμε μεγαλεπήβολα πληροφοριακά συστήματα τα οποία μπορούν να παρέχουν τις υπηρεσίες τους παγκοσμίως.

Όπως είδαμε και στο κεφάλαιο περί διαχείρισης κινδύνου, το συγκεκριμένο πεδίο προήλθε και αυτό από κάπου αλλού και δεν επινοήθηκε για τις ανάγκες τις πληροφορικής. Παρόλα αυτά, η έρευνα που πραγματοποιήθηκε στο συγκεκριμένο πεδίο μάλλον πως ήταν εξαιρετικά ενδελεχής και ποιοτική, αν αναλογιστούμε το γεγονός πως η μεθοδολογία EBIOS παρουσιάστηκε το 1995 και χρησιμοποιείται ακόμα. Η σύνδεση της διαχείρισης κινδύνου με τα πληροφοριακά συστήματα είναι κρίσιμης σημασίας καθώς μας βοηθά να αποτιμήσουμε τα διάφορα στοιχεία του πληροφοριακού συστήματος και να προβλέψει εν μέρει τις συνέπειες ενός περιστατικού ασφαλείας. Έτσι γίνεται δυνατή η καλύτερη διαχείριση των περιστατικών από οργανωτικής απόψεως, συνεπώς η οικονομική ζημιά ελαχιστοποιείται. Το εργαλείο της EBIOS ίσως να έχει παλιώσει και το γραφικό του περιβάλλον να θεωρείται αρχαίο, δεν έχει όμως τίποτα να ζηλέψει από άλλα εργαλεία διαχείρισης κινδύνου καθώς μπορεί να βοηθήσει τον αναλυτή κινδύνου καθ΄ όλη την διάρκεια της διαδικασίας διαχείρισης κινδύνου.

Στην συνέχεια εξετάσαμε την SecureTropos μία σχετικά ώριμη μεθοδολογία σχεδίασης συστημάτων με γνώμονα την ασφάλεια. Στην μεθοδολογία αναφέρθηκαν όλοι οι ορισμοί που μπορούν να χρησιμοποιηθούν κατά την διάρκεια διαχείρισης κινδύνου, κάτι το οποίο κατέστησε πολύ εύκολη την διασύνδεση αυτών των δύο διαδικασιών. Διάφοροι οργανισμοί ανά τον κόσμο συνειδητοποίησαν πως είναι φθηνότερο να σχεδιάζεις ένα ασφαλές σύστημα, παρά να προσπαθείς να αντιμετωπίζεις όλα τα περιστατικά ασφαλείας που συμβαίνουν, την στιγμή της εμφάνισής τους, κάτι το οποίο αντικατοπτρίζεται εν μέρει στην ζήτηση που υπάρχει στην αγορά για επαγγελματίες του χώρου της κυβερνοασφάλειας. Με το εργαλείο SecTro, οι εφευρέτες της SecureTropos προσφέρανε πολύ καλό

εργαλείο στους αναλυτές για να σχεδιάσουν ασφαλειοστραφή συστήματα, το οποίο ανανεώνεται και βελτιώνεται συνεχώς.

Η μεθοδολογία Pris είναι λιγότερο ώριμη από την SecureTropos αλλά εξίσου σημαντική. Το κενό που υπήρχε στον ακαδημαϊκό χώρο, στο πεδίο που ασχολούταν με την ιδιωτικότητα κατά την σχεδίαση συστημάτων καλύφθηκε. Η ύπαρξη ενός εργαλείου θα ήταν κάτι το οποίο θα βοηθούσε ακόμα περισσότερο τους σχεδιαστές συστημάτων, δυστυχώς όμως δεν υφίσταται κάτι τέτοιο. Παρόλα αυτά η βοήθεια που μπορεί να προσφέρει δεν είναι σε καμία περίπτωση αμελητέα καθώς ως μεθοδολογία είναι πλήρης ως προς τους σκοπούς που προσπαθεί να εκπληρώσει.

Σχόλιο [C15]: Μα και BEBAIA μας προβληματιζει η ιδιωτικοτητα.

Η μεθοδολογία SaferTec είναι η αιχμή του δόρατος όσον αφορά την ανάλυση συστημάτων και την ενσωμάτωση των όποιων στόχων ασφαλείας και ιδιωτικότητας σε οποιοδήποτε πληροφοριακό σύστημα. Η modular φύση του, επιτρέπει την χρήση διάφορων μεθοδολογιών οι οποίες αποσκοπούν στον ίδιο σκοπό κάτι το οποίο την κάνει πλήρως ευέλικτη και κατανοητή από τους αναλυτές.

7.2 Μελλοντική έρευνα

Όπως είδαμε και στο κεφάλαιο έξι και πιο συγκεκριμένα στο σύστημα C-ITS-S, τα cloud συστήματα πλέον χρησιμοποιούνται σε τέτοιο βαθμό από τις υποδομές μιας εφαρμογής που τείνουν να γίνουν standard. Η ευέλικτη φύση τους, η αξιοποίηση των πόρων που πραγματοποιείται και οι συνεχώς αναδυόμενες τεχνολογίες που σχετίζονται με την νεφοϋπολογιστική, υποστηρίζουν και δικαιολογούν αυτή την τάση της βιομηχανίας. Πιο συγκεκριμένα, για να υποστηρίξουμε τα λεγόμενά μας, έρευνα του insight.com υποστηρίζει πως τα χρήματα που δαπανήθηκαν το 2015 ήταν 25 δις δολάρια και το 2016 αυτή η τιμή άγγιξε τα 38 δις. Επίσης κάτι το οποίο δεν περιμέναμε να βρούμε στην συγκεκριμένη έρευνα, αναφέρει πως το δεύτερο μεγαλύτερο πρόβλημα που αντιμετωπίζει η βιομηχανία όταν αναλογίζεται την υιοθεσία αρχιτεκτονικής σύννεφου είναι η ασφάλεια (25). Συνεπώς η ασφάλεια και η ιδιωτικότητα των νεφοϋπολογιστικών συστημάτων, θα πρέπει να είναι αυτή που θα πρέπει να απασχολήσει την ακαδημαϊκή κοινότητα, αλλά και τον συγγραφέα αν αυτός αποφασίσει να προχωρήσει την ακαδημαϊκή του καριέρα.

Σχόλιο [C16]: Εμμ.. Ναι... Οοοοοοοοοοχι.

Πηγές

1. IETF. RFC 2828. [Ηλεκτρονικό] https://www.ietf.org/rfc/rfc2828.txt.

2. NIST. Standards for Security Categorization of Federal Information and Information Systems. [Ηλεκτρονικό] http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf.

3. K., Lambrinoudakis. Privacy Enhancing Technologies, Course notes - Lesson 1.

4. IETF. Privacy Terminology. [Ηλεκτρονικό] https://tools.ietf.org/id/draft-hansen-privacy-terminology-00.html.

5. ISO99. Common Criteria for Information Technology Security Evaluation. [Ηλεκτρονικό]

6. Bertalanffy, Ludwig von. *General Systems Theory.* 1968.

7. Sommerville, Ian. *Software Engineering, 9th Edition.*

8. *iso27001security.* [Ηλεκτρονικό] http://www.iso27001security.com/html/risk_mgmt.html#ResidualRisk.

9. *Comparative study of information security risk assessment models.* Filipe Macedo, Miguel Mira da Silva.

10. Security, U.S. Department of Homeland. Understanding Risk Communication Theory: A Guide for Emergency Managers and Communicators. [Ηλεκτρονικό] http://www.start.umd.edu/sites/default/files/files/publications/UnderstandingRiskCommunicationTheory.pdf.

11. Risk Monitoring. *dot.state.cmn.us.* [Ηλεκτρονικό] www.dot.state.mn.us/pm/documents/guidance/risk-monitoring2.docx.

12. Enisa. Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools.

13. ENISA. Risk Treatment. *enisa.europa.eu.* [Ηλεκτρονικό] https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-process/risk-treatment.

14. Anderson, R. *Security Engineering: A Guide to Building Dependable Distributed Systems.* 2001.

15. Haralambos Mouratidis, Paolo Giorgini. *Secure Tropos: A security-oriented extension of the tropos methodology.*

16. *The Tropos methodology: An overview.* Paolo Giorgini, Manuel Kolp, John Mylopoulos, Marco Pistore.

17. *Tropos: An agent-oriented software development methodology.* Paolo Bresciani, Anna Perini, Paolo Giorgini, Fausto Giunchiglia, John Mylopoulos.

18. *SecTro: A CASE Tool for Modelling Security in Requirements Engineering using Secure Tropos.* Michalis Pavlidis, Shareeful Islam.

19. Stefanos, Gritzalis. Enhancing Web privacy and anonymity in the digital era.

20. *Privacy Enhancing Technologies.* Koorn, van Gils, Hart, Overbreek, Tellegen.

21. *Addressing privacy requirements in system design: The Pris method.* Kalloniatis, Kavakli, Gritzalis.