ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗ ΜΕ ΕΦΑΡΜΟΓΕΣ ΣΤΗ ΒΙΟΪΑΤΡΙΚΗ

"Μελέτη, σχεδίαση και υλοποίηση μεθοδολογιών ανάπτυξης και διαχείρισης της επικινδυνότητας ενός Πληροφοριακού Συστήματος"

ΦΟΙΤΗΤΡΙΑ: ΓΚΟΣΔΗ ΜΑΡΙΑ
Α.Μ: 368

ΕΠΙΒΛΕΠΩΝ: ΦΟΙΒΟΣ ΜΥΛΩΝΑΣ,
ΕΠΙΚΟΥΡΟΣ ΚΑΘΗΓΗΤΗΣ

ΣΕΠΤΕΜΒΡΙΟΣ 2014

Τριμελής επιτροπή:

Κος Μυλωνάς Φοίβος – Απόστολος
Κος Σανδαλίδης Χαρίλαος
Κος Αναγνωστόπουλος Ιωάννης

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΕΡΙΛΗΨΗ

Καθώς οι περισσότεροι οργανισμοί βασίζουν ένα μεγάλο μέρος της λειτουργίας τους σε πληροφοριακά συστήματα, η ανάγκη για κατάλληλη ασφάλεια αυξάνεται. Δυστυχώς, είναι δύσκολο να γίνει επιλογή των μέτρων ασφάλειας ώστε να επιτευχθεί ικανοποιητική ασφάλεια. Μεγάλες ποσότητες πόρων ξοδεύονται με βάση την αποφυγή των αποτυχιών. Παρόλα αυτά είναι αδύνατο να υπάρξει η εγγύηση ότι το πληροφοριακό σύστημα είναι τέλειο. Αυτό που όμως είναι δυνατό να επιτευχθεί είναι η μείωση της πιθανότητας εμφάνισης κινδύνου. Προϋπόθεση για την επίτευξη αυτής της μείωσης είναι η εφαρμογή μιας κατάλληλης διαχείρισης επικινδυνότητας ώστε να επιτευχθεί επαρκής αναγνώριση και αποτελεσματική αντιμετώπιση των κινδύνων που απειλούν το σύστημα.

Η εργασία αυτή ασχολείται με την ανάλυση και τη διαχείριση της επικινδυνότητας ενός πληροφοριακού συστήματος. Αρχικά, παρουσιάζονται και αναλύονται κάποιες βασικές έννοιες σχετικά με τον κίνδυνο και τη διαχείρισή του στα πληροφοριακά συστήματα. Έπειτα, περιγράφεται το πρότυπο ISO, καθώς και οι κυριότερες μεθοδολογίες για την αξιολόγηση και διαχείριση της επικινδυνότητας στα πληροφοριακά συστήματα. Τέλος, παρουσιάζεται ένα εργαλείο ανοικτού κώδικα, το EBIOS, που χρησιμοποιήθηκε για την εξαγωγή και αξιολόγηση συμπερασμάτων αναφορικά με το σύνολο των υπολογιστικών μονάδων του τμήματος Πληροφορική με εφαρμογές στη Βιοϊατρική του Πανεπιστημίου Θεσσαλίας.

ΘΕΩΡΗΤΙΚΟ ΜΕΡΟΣ

Κεφάλαιο 1 ΕΙΣΑΓΩΓΗ

1.1 ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Στον όρο « Ασφάλεια» μπορούν να αποδοθούν πολλές ερμηνείες, κάθε μία από τις οποίες μπορεί να αποδώσει με ακρίβεια διαφορετικές καταστάσεις. Σύμφωνα με τον ορισμό του λεξικού της Οξφόρδης, «ασφάλεια είναι η ελευθερία από τον κίνδυνο ή το φόβο». Διάφοροι άλλοι ορισμοί μπορούν να χρησιμοποιηθούν για να προσδιορίσουν την ασφάλεια όπως :

- Η κατάσταση στην οποία δεν υπάρχουν κίνδυνοι, όπου αισθάνεται κανείς ότι δεν απειλείται.
- Η αποτροπή κινδύνου ή απειλής, η εξασφάλιση σιγουριάς και βεβαιότητας.
- Υπηρεσία της Αστυνομίας.
- Η λεκτική διάταξη που αποτρέπει πιθανά ατυχήματα.
- Μηχανισμός στην πόρτα αυτοκινήτου.
- Συμφωνία μεταξύ ασφαλιστικής εταιρείας και πελάτη.
- Ιατροφαρμακευτική περίθαλψη.

Από μία άποψη, η ασφάλεια μπορεί να έγκειται στην επαρκή προστασία ανθρώπων και αγαθών, για την οποία μπορεί να λαμβάνονται διάφορα μέτρα προστασίας από πιθανούς κινδύνους. Για παράδειγμα, η φυσική ασφάλεια ενός κτιρίου έγκειται στην αποτροπή εισόδου κακόβουλων ατόμων και στην αποτροπή ζημιών από φυσικές καταστροφές. Αντίστοιχα, η ασφάλεια μίας ηλεκτρονικής βάσης δεδομένων έγκειται στην προστασία των δεδομένων από καταστροφή, διαγραφή, αλλοίωση ή αποκάλυψη σε μη εξουσιοδοτημένους χρήστες.

Η επιστήμη της ασφάλειας υπολογιστών σχετίζεται με ένα πλήθος γνωστικών αντικειμένων, θεωριών και τεχνολογιών που έχουν ως σκοπό την πρόληψη, την ανίχνευση και αντιμετώπιση μη εξουσιοδοτημένων πράξεων, οι οποίες σχετίζονται με τη χρήση υπολογιστικών συστημάτων.

Ο ρόλος του ηλεκτρονικού υπολογιστή κατά την εκτέλεση των μη εξουσιοδοτημένων πράξεων συνήθως είναι διττός :

- Αποτελεί βασικό εργαλείο για την εκτέλεσή τους
- Ο ίδιος ο ηλεκτρονικός υπολογιστής, και συγκεκριμένα τα δεδομένα ή και οι πληροφορίες που περιέχονται ή δημιουργούνται σε αυτόν, αποτελεί στόχο των πράξεων αυτών.

Οι μη εξουσιοδοτημένες πράξεις, ανάλογα με τις συνέπειές τους μπορούν να αποτελούν ή όχι ηλεκτρονικό έγκλημα (e-crime, computer crime).

Το ηλεκτρονικό έγκλημα ορίζεται από τους Forester και Morrison το 1994 ως :

«Μία εγκληματική πράξη κατά την εκτέλεση της οποίας ο ηλεκτρονικός υπολογιστής αποτελεί το βασικό εργαλείο».
Η ασφάλεια υπολογιστών χρησιμοποιεί τη γνώση που πηγάζει από τη μελέτη αρκετών γνωστικών χώρων, όχι απαραίτητα αλληλοσχετιζόμενων, όπως Πληροφορική, Κρυπτογραφία και Κοινωνικές Επιστήμες.

1.2 ΑΠΑΙΤΗΣΕΙΣ ΑΣΦΑΛΕΙΑΣ

Μία αναγκαία συνθήκη για να είναι δυνατή η αποτίμηση της ασφάλειας είναι η ύπαρξη κάποιου συνόλου απαιτήσεων, που πρέπει να αντιστοιχούν σε κάποια θεμελιώδη χαρακτηριστικά, με την έννοια ότι κανένα από αυτά δεν πρέπει να απουσιάζει ή να αγνοηθεί. Έτσι ενώ μπορεί να δίνεται μεγαλύτερη ή μικρότερη βαρύτητα σε κάποιο από αυτά, ανάλογα με την περίπτωση, τελικά όλα πρέπει να λαμβάνονται υπόψη. Τα χαρακτηριστικά που είναι κοινά αποδεκτά είναι η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα.

- Εμπιστευτικότητα (confidentiality) : προστασία από το να έχουν πρόσβαση μη εξουσιοδοτημένα λογικά ή φυσικά αντικείμενα (π.χ. προγράμματα, άνθρωποι)
- Ακεραιότητα (integrity) : είναι η ιδιότητα των στοιχείων του συστήματος (κυρίως δεδομένων) να είναι ακριβή και να αντιπροσωπεύουν την πραγματικότητα. Συνέπεια της ακεραιότητας είναι κάθε αλλαγή (π.χ. του περιεχομένου των δεδομένων) να είναι αποτέλεσμα εξουσιοδοτημένης ενέργειας ενώ, παράλληλα, μη εξουσιοδοτημένη αλλαγή να μην είναι δυνατή.

- Διαθεσιμότητα (availability) : είναι η ιδιότητα των πόρων του συστήματος να καθίστανται αμέσως προσπελάσιμοι από κάθε εξουσιοδοτημένο λογικό ή φυσικό αντικείμενο, που απαιτεί παρόμοια πρόσβαση.

Δύο ακόμα σημαντικές έννοιες είναι οι εξής :

- Αυθεντικότητα (authenticity) : η αποφυγή ατελειών και ανακριβειών κατά τη διάρκεια των εξουσιοδοτημένων τροποποιήσεων μιας πληροφορίας.

- Εγκυρότητα (validity) : η απόλυτη ακρίβεια και πληρότητα μιας πληροφορίας.

Η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα αποτελούν τους τρεις κύριους επιδιωκόμενους στόχους στην ασφάλεια πληροφοριακών

συστημάτων. Μερικές φορές αλληλεπικαλύπτονται, ενώ άλλες φορές είναι αμοιβαία αποκλειόμενες. Για παράδειγμα, ισχυρή προστασία της εμπιστευτικότητας μπορεί να περιορίσει σε μεγάλο βαθμό τη διαθεσιμότητα, και το αντίστροφο.

1.3 ΤΡΟΠΟΙ ΠΑΡΑΒΙΑΣΗΣ ΠΛΗΡΟΦΟΡΙΑΚΟΥ ΣΥΣΤΗΜΑΤΟΣ

Οι παραβιάσεις πραγματοποιούνται αν υπάρχουν ταυτόχρονα μία απειλή για το σύστημα και μία αδυναμία του συστήματος. Υπάρχουν τέσσερις τρόποι με τους οποίους μπορεί να παραβιαστεί ένα πληροφοριακό σύστημα. Καθένας από αυτούς καταργεί μία ή περισσότερες εκ των παραμέτρων που καθορίζουν εάν ένα σύστημα είναι ασφαλές.

- Υποκλοπή (interception) : μία μη εξουσιοδοτημένη οντότητα έχει αποκτήσει πρόσβαση σε κάποια πληροφορία. Η οντότητα αυτή μπορεί να είναι ένα άτομο, ένα πρόγραμμα ή ακόμα και ένα υπολογιστικό σύστημα. Παράδειγμα τέτοιας παραβίασης είναι η παράνομη αντιγραφή προγραμμάτων ή αρχείων καθώς και η υποκλοπή δεδομένων σε δίκτυο. Είναι επομένως φανερό ότι με την παραβίαση αυτή καταργείται άμεσα η εμπιστευτικότητα των δεδομένων.

- Παρεμβολή (interruption): ένα στοιχείο του συστήματος χάνεται ή αχρηστεύεται. Παράδειγμα είναι η σκόπιμη καταστροφή μιας συσκευής hardware ή το σβήσιμο ενός προγράμματος ή αρχείου. Στην περίπτωση αυτή χάνεται η διαθεσιμότητα των πληροφοριών.

- Τροποποίηση (modification) : μία μη εξουσιοδοτημένη οντότητα έχει αποκτήσει πρόσβαση σε κάποια πληροφορία και την έχει αλλοιώσει. Για παράδειγμα, κάποιος μπορεί να αλλοιώσει στοιχεία μιας βάσης δεδομένων, να τροποποιήσει ένα πρόγραμμα ώστε αυτό να εκτελεί έναν επιπλέον υπολογισμό ή ακόμα και να κάνει μετατροπές στο υλικό (hardware). Κάποιες από τις παραπάνω ενέργειες είναι εμφανείς, όμως άλλες πιο περίπλοκες είναι σχεδόν αδύνατο να ανιχνευθούν. Δηλαδή παύει να υφίσταται όχι μόνο η εμπιστευτικότητα των πληροφοριών, αλλά και η ακεραιότητα και η εγκυρότητά τους.

- Πλαστογράφηση (fabrication) : είναι δυνατή η πλαστογράφηση αντικειμένων με τη βοήθεια ενός πληροφοριακού συστήματος. Αυτό μπορεί να γίνει με προσθήκη αρχείων σε μία βάση δεδομένων. Σε πολλές περιπτώσεις είναι αδύνατο να ξεχωρίσει κανείς αν το αντικείμενο είναι

γνήσιο ή όχι. Με τον τρόπο αυτό καταργείται η εμπιστευτικότητα και η εγκυρότητα των δεδομένων.

1.4 ΤΡΟΠΟΙ ΑΝΤΙΜΕΤΩΠΙΣΗΣ

Είναι φανερό ότι οι συνέπειες πραγματοποίησης μιας παραβίασης σε ένα πληροφοριακό σύστημα είναι εξαιρετικά βλαβερές. Για την αποφυγή λοιπόν των ιδιαίτερα δυσμενών επιπτώσεων που μπορούν να υπάρξουν, κρίνεται σκόπιμο να εφαρμοστούν μέτρα προστασίας των πληροφοριακών συστημάτων. Τα μέτρα αυτά αποσκοπούν στην προφύλαξη των πληροφοριακών συστημάτων από τις εξωτερικές απειλές και τις ενδογενείς αδυναμίες τους, καθώς και από κακόβουλες ενέργειες που ενδέχεται να οδηγήσουν σε παραβίαση των πληροφοριακών συστημάτων. Τα κυριότερα μέτρα προστασίας είναι τα εξής :

- Κρυπτογράφηση : είναι το ισχυρότερο εργαλείο στην ασφάλεια των πληροφοριακών συστημάτων. Μετατρέποντας τα δεδομένα σε μη αναγνώσιμη μορφή, σχεδόν εκμηδενίζεται ο κίνδυνος υποκλοπής ή αλλοίωσής τους. Επίσης, σε ορισμένα πρωτόκολλα η κρυπτογράφηση χρησιμοποιείται για τη διάθεση πληροφοριών σε εξουσιοδοτημένους χρήστες. Δηλαδή η κρυπτογράφηση εξασφαλίζει σε μεγάλο βαθμό τους τρεις βασικούς στόχους της ασφάλειας. Δεν πρέπει όμως να υπερεκτιμηθεί η αξία της. Πρέπει να γίνει κατανοητό ότι η κωδικοποίηση, εφόσον δεν υλοποιείται κατάλληλα, δεν βελτιώνει την επίδοση του συστήματος στο θέμα της ασφάλειας. Αντίθετα, μπορεί να επιφέρει το αντίθετο αποτέλεσμα αφού δίνει μία ψευδή αίσθηση ασφάλειας χωρίς όμως να μπορεί στην πράξη να εγγυηθεί κάτι τέτοιο.

- Έλεγχοι λογισμικού : υπάρχουν τρεις κατηγορίες τέτοιων ελέγχων. Πρώτον, ο εσωτερικός έλεγχος όπου τα τμήματα του προγράμματος ενισχύουν την ασφάλεια του συστήματος. Τέτοιο παράδειγμα είναι ο έλεγχος πρόσβασης σε ένα πρόγραμμα διαχείρισης βάσεων δεδομένων. Δεύτερον ο έλεγχος του λειτουργικού συστήματος. Το λειτουργικό σύστημα επιβάλλει περιορισμούς ώστε ο κάθε χρήστης να προστατεύεται από τους υπόλοιπους. Τέλος, οι έλεγχοι ανάπτυξης. Αυτοί περιλαμβάνουν κριτήρια ποιότητας βάση των οποίων σχεδιάζεται, κωδικοποιείται, ελέγχεται και συντηρείται ένα πρόγραμμα.

- Έλεγχοι υλικού : οι έλεγχοι αυτοί είναι πολυάριθμοι και μπορεί να περιλαμβάνουν κλειδαριές, αντικλεπτικά συστήματα, συσκευές αναγνώρισης στοιχείων χρήστη κλπ.

- Πολιτικές : η συχνή αλλαγή κωδικών πρόσβασης (passwords), η εκπαίδευση του προσωπικού, η θέσπιση ηθικού κώδικα για τους επαγγελματίες των υπολογιστών είναι οι συνηθέστερες πολιτικές που χρησιμοποιούνται για την προστασία των πληροφοριών.

- Φυσικοί έλεγχοι : είναι οι πιο εύκολοι, οικονομικοί αλλά και πολλές φορές οι πιο αποτελεσματικοί έλεγχοι. Περιλαμβάνουν κλειδαριές, φρουρούς, εφεδρικά αντίγραφα ασφαλείας των σημαντικών εγγράφων και δεδομένων, αλλά και σχεδιασμό αντιμετώπισης εκτάκτων περιστατικών που να καλύπτει τις φυσικές καταστροφές.

Η αποτελεσματικότητα των παραπάνω ελέγχων είναι συνάρτηση αρκετών παραμέτρων, βασικότερη των οποίων είναι η συνειδητοποίηση του προβλήματος. Πολλοί χρήστες δεν υπακούν στους κανόνες ασφάλειες, αφού δεν είναι πεπεισμένοι για την αναγκαιότητα ύπαρξης των μέτρων αυτών. Επίσης, είναι σημαντικό να είναι οι έλεγχοι σαφείς, προσαρμοσμένοι στο εκάστοτε σύστημα και να μην απαιτούν πολύ χρόνο και πόρους για την πραγματοποίησή τους. Επιπλέον, η ταυτόχρονη διεξαγωγή διαφορετικών ελέγχων στο ίδιο σύστημα αυξάνει σημαντικά την απόδοση τους σε σχέση με τη διεξαγωγή καθενός μεμονωμένα. Ζωτικής σημασίας είναι και η περιοδική αναθεώρηση των ελέγχων. Ο κύκλος ζωής τους είναι περιορισμένος, αφενός γιατί το ίδιο συμβαίνει και στο υπό προστασία σύστημα (π.χ. το λογισμικό συνεχώς αναβαθμίζεται), αφετέρου γιατί οι απειλές είναι ολοένα και πιο έντονες (π.χ. ο ανταγωνισμός ενισχύει την προσπάθεια του να παραβιάσει το σύστημα). Τέλος, θα πρέπει τα συστήματα να είναι σχεδιασμένα ώστε να είναι ανεκτικά σε σφάλματα, δηλαδή να διατηρείται η ασφάλεια των πληροφοριακών συστημάτων παρά τις δυσλειτουργίες ορισμένων συνθετικών τους. Αυτή η ιδιότητα ενισχύει σημαντικά την άμυνα των πληροφοριακών συστημάτων απέναντι σε εσωτερικές τεχνικές αδυναμίες.

Με την εφαρμογή των παραπάνω μέτρων προστασίας, οι εμπλεκόμενοι φορείς καλούνται να διατηρήσουν την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των πληροφοριακών συστημάτων.

Κεφάλαιο 2 ΔΙΑΧΕΙΡΙΣΗ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ (RISK MANAGEMENT)

Η διαχείριση της επικινδυνότητας αποτελείται από τρεις άξονες :

- Την ανάλυση επικινδυνότητας
- Την μείωση των κινδύνων
- Τον έλεγχο ασφάλειας πληροφοριακού συστήματος

2.1 ΑΝΑΛΥΣΗ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ

Η ανάλυση επικινδυνότητας είναι μία « οργανοτεχνική μελέτη η οποία μελετά τις απειλές, τις ευπάθειες και τα αγαθά ενός οργανισμού και προτείνει τα μέτρα ασφάλειας που πρέπει να ληφθούν για την αντιμετώπιση των προσδιορισμένων απειλών ». Στην πράξη ο κίνδυνος είναι ένα μέτρο της πιθανότητας πραγματοποίησης ενός συγκεκριμένου ανεπιθύμητου γεγονότος και είναι άμεσα συνδεδεμένος με ένα ή περισσότερα στοιχεία του συστήματος. Αυτή η πιθανότητα εξαρτάται τόσο από την πιθανότητα πραγματοποίησης της επίθεσης όσο και από την πιθανότητα της επιτυχίας της, η οποία ακολούθως εξαρτάται από την επιτυχή εκμετάλλευση των αδυναμιών του συστήματος. Η διαδικασία αποτίμησης του κινδύνου λαμβάνει υπόψη τόσο την πιθανότητα πραγματοποίησης της απειλής, όσο και την επίπτωση που θα έχει στο πληροφοριακό σύστημα προκειμένου να εκτιμήσει τον βαθμό εκείνο στον οποίο ο κίνδυνος πρέπει να μειωθεί με κατάλληλα μέτρα. Η αξία αποτίμησης βάσει του κινδύνου (risk-based reasoning) έγκειται στο ότι παρέχει κριτήρια αποφάσεων για τις απαιτήσεις ασφάλειας (security requirements) εν μέσω του επιχειρησιακού και κοινωνικού περιβάλλοντος. Η αποτίμηση κινδύνων αναγνωρίζεται καθολικά σαν η μόνη βιώσιμη μέθοδος για την τεκμηρίωση των μέτρων ασφάλειας σε όρους κόστους – ωφέλειας, ή για την εκλογή των αποδοτικότερων αντιμέτρων. Σαν συνέπεια, η διαχείριση κινδύνων είναι η βάση των περισσότερων εθνικών προτύπων για διαχείριση ασφάλειας πληροφοριών π.χ.BSI-EN 2002 και βέλτιστες πρακτικές π.χ. BSI-EN 2001. Παρά την ύπαρξη διαφορετικών βαθμών ελευθερίας στην εκλογή των μεθοδολογιών για την εκπόνηση μιας μελέτης ανάλυσης επικινδυνότητας, τα πρότυπα ακολουθούν τα ίδια βασικά βήματα για τη διαχείριση των κινδύνων :

1. Ορισμός του περιβάλλοντος και των ορίων του πληροφοριακού συστήματος
2. Εντοπισμός των αγαθών του πληροφοριακού συστήματος και ανεπιθύμητες καταστάσεις που ενδέχεται να προκύψουν σε αυτά τα αγαθά
3. Αποτίμηση των κινδύνων κάθε απειλής για κάθε αγαθό, λαμβάνοντας υπόψη πιθανές επιθέσεις και αδυναμίες

4. Εκλογή κατάλληλων αντιμέτρων
5. Υλοποίηση, εφαρμογή και περιοδική επανα-αποτίμηση του επιπέδου κινδύνου.

Οι διαφορές μεταξύ των προσεγγίσεων διαχείρισης κινδύνων περιλαμβάνουν τον τρόπο ποσοτικοποίησης των κινδύνων, τον προσανατολισμό της προσέγγισης σε αποτίμηση βασισμένη σε αγαθά (asset-based approaches) ή σε διεργασίες πληροφορικής (process-based approaches) και το επίπεδο γνώσεων και εξειδίκευσης που απαιτείται από τον ειδικό ασφάλειας για την εφαρμογή των αντιμέτρων.

2.2 ΜΕΙΩΣΗ ΤΩΝ ΚΙΝΔΥΝΩΝ

Η μείωση των κινδύνων είναι μία συστηματική μεθοδολογία που υιοθετείται από τη διοίκηση προκειμένου να μειώσει το επίπεδο του κινδύνου για τον οργανισμό σε αποδεκτά επίπεδα. Αποτελείται από μία σειρά ενεργειών που εμπλέκουν θέσπιση προτεραιοτήτων, αξιολόγηση και υλοποίηση των κατάλληλων αντιμέτρων που προκύπτουν από την ανάλυση επικινδυνότητας. Με δεδομένο ότι η εξάλειψη όλων των κινδύνων είναι συνήθως μη εφαρμόσιμη ή σχεδόν αδύνατη, η διοίκηση και οι επικεφαλείς των επιχειρησιακών μονάδων ενός οργανισμού έχουν την ευθύνη για την υιοθέτηση της πιο οικονομικής λύσης και την υλοποίηση των καταλληλότερων αντιμέτρων προκειμένου να μειώσουν τον κίνδυνο σε ένα αποδεκτό επίπεδο, με την μικρότερη δυνατή επίδραση στους πόρους και τη στρατηγική επιστολή του οργανισμού. Τα κύρια θέματα της μείωσης των κινδύνων είναι :

1. οι διαθέσιμες επιλογές για την μείωση των κινδύνων (risk mitigation options)
2. η στρατηγική που θα υιοθετήσει (risk mitigation strategy)
3. η υλοποίηση των αντιμέτρων (control implementation)
4. οι διαφορετικές κατηγορίες των αντιμέτρων (control categories)
5. η ανάλυση κόστους – ωφέλειας για την αιτιολόγηση των επιλεγμένων αντιμέτρων (cost – benefit analysis)
6. ο εναπομένων κίνδυνος (residual risk).

Αυτό μπορεί να επιτευχθεί με :

- αποδοχή του κινδύνου
- αποφυγή του κινδύνου
- μείωση του κινδύνου
- κατάρτιση σχεδίου μείωσης κινδύνου
- έρευνα για τρόπους διόρθωσης της αδυναμίας που προκαλεί κίνδυνο
- μεταφορά του κινδύνου σε τρίτα μέρη.

Με δεδομένο ότι οι στόχοι ενός οργανισμού καθορίζουν και τη λειτουργία του δεν υπάρχει ένας μόνος τρόπος για την μείωση του κινδύνου. Οι κυριότερες κατηγορίες των μέτρων είναι :

1. τεχνικά μέτρα ασφάλειας που στοχεύουν στα τεχνικά χαρακτηριστικά των πόρων και χωρίζονται σε
    - υποστηρικτικά (όπως είναι η ταυτοποίηση, η διαχείριση κρυπτογραφικών κλειδιών, η διαχείριση ασφάλειας, οι βέλτιστες λειτουργικές πρακτικές),
    - προληπτικά (όπως είναι η αυθεντικοποίηση, η ταυτοποίηση, η επιβολή ελέγχου πρόσβασης, η μη – αποποίηση ευθύνης, οι προστατευμένες επικοινωνίες, η μυστικότητα συναλλαγής) και
    - διαγνωστικά (όπως είναι ο έλεγχος, η ανίχνευση και ο περιορισμός των εισβολών, η ακεραιότητα, τα σημεία επαναφοράς σε συστημική κατάσταση, η ανίχνευση και η εξάλειψη ιομορφικού λογισμικού).

2. διαδικαστικά μέτρα ασφάλειας που δίνουν έμφαση στην τήρηση των πολιτικών, προτύπων και διαδικασιών και χωρίζονται σε
    - Προληπτικά (όπως είναι ο καθορισμός ρόλων και υπευθυνοτήτων, η ανάπτυξη σχεδίων ασφάλειας, οι διαδικασίες πρόσβασης και διαχείρισης αλλαγών, η επιμόρφωση και εκπαίδευση σε θέματα ασφάλειας)
    - Διαγνωστικά (όπως είναι η υλοποίηση μέτρων ασφάλειας για τους χρήστες, οι περιοδικοί έλεγχοι ασφάλειας, οι διαδικασίες διαχείρισης κινδύνων)
    - Ανάκτησης λειτουργιών (όπως είναι η μονάδα διαχείρισης περιστατικών ασφάλειας)

3. λειτουργικά μέτρα ασφάλειας που δίνουν έμφαση στην τήρηση των ελάχιστων αποδεκτών τεχνοδιαμορφώσεων με κατάρτιση αναλυτικών οδηγών και διαδικασιών και χωρίζονται σε
    - Προληπτικά (όπως είναι το ιομορφικό λογισμικό, οι διαδικασίες πρόσβασης)
    - Διαγνωστικά (όπως είναι η φυσική ασφάλεια).

2.3 ΕΛΕΓΧΟΣ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΑΚΟΥ ΣΥΣΤΗΜΑΤΟΣ

Η ανάλυση επικινδυνότητας αποτελεί σημαντικό παράγοντα στο σχεδιασμό του ελέγχου, μέσω του εντοπισμού κινδύνων και ευπαθειών, ο ελεγκτής είναι σε θέση να προσδιορίσει τους απαραίτητους μηχανισμούς ελέγχου έτσι ώστε να περιορίσει αυτούς τους κινδύνους

σε ένα αποδεκτό επίπεδο. Επίσης, ο ελεγκτής πρέπει να είναι σε θέση να προσδιορίσει και να διακρίνει επαρκώς τους διαφορετικούς τύπους κινδύνων, καθώς και την σπουδαιότητα και την επάρκεια των αντίστοιχων μέτρων ασφάλειας. Η εκτίμηση αυτή δεν πρέπει να γίνεται μόνο σε τεχνικό επίπεδο αντιμέτρων αλλά και σε επίπεδο επιχειρησιακών λειτουργιών. Ο ελεγκτής μέσω της ανάλυσης επικινδυνότητας έχει τη δυνατότητα να κατηγοριοποιήσει και να εντοπίσει τους σημαντικότερους κινδύνους για το πληροφοριακό σύστημα. Λόγω των περιορισμένων τεχνολογικών και ανθρώπινων πόρων, συχνά είναι ανέφικτη η πραγματοποίηση ενδελεχών ελέγχων για την αντιμετώπιση όλων των πιθανών κινδύνων, έτσι ο ελεγκτής οδηγείται σε μία επιλογή ελεγκτικών στόχων, τόσο ποσοτική όσο και ποιοτική. Σε αυτήν τη δύσκολη διαδικασία έχει σαν βοηθό την ανάλυση επικινδυνότητας.

Από την άλλη πλευρά του ελέγχου του πληροφοριακού συστήματος, η ανάλυση επικινδυνότητας έχει τα εξής πλεονεκτήματα για τον σχεδιασμό του:

1. Αποτελεσματική κατανομή των ελεγκτικών πόρων
2. Διαβεβαίωση ότι είναι διαθέσιμη μία αντιπροσωπευτική εικόνα του οργανισμού και του πληροφοριακού συστήματος λαμβάνοντας πληροφορίες από όλα τα επίπεδα του οργανισμού
3. Παροχή μιας αφετηρίας για αποτελεσματική διαχείριση του τμήματος εσωτερικού ελέγχου
4. Σύνδεση του συγκεκριμένου αντικειμένου ελέγχου με τον οργανισμό.

2.4 ΤΥΠΟΣ BPL

Καρδιά της ανάλυσης κινδύνων είναι ο τύπος
B > P * L όπου:

- B είναι το κόστος για την πρόληψη μιας απώλειας
- P είναι η πιθανότητα να συμβεί μία απώλεια
- L είναι το συνολικό κόστος μιας απώλειας

Ο τύπος αυτός αποτελεί την κεντρική ιδέα πίσω από κάθε ανάλυση κινδύνων, την ιδέα του υπολογισμού της πιο συμφέρουσας λύσης. Ωστόσο αν και ο υπολογισμός του τύπου και πρακτική του εφαρμογή βρίσκουν σημαντικές δυσκολίες, όλες οι μέθοδοι ανάλυσης των κινδύνων βασίζονται πάνω στη λογική του τύπου BPL.

Το νόημα του τύπου είναι όταν το κόστος της πρόληψης μιας απώλειας είναι μεγαλύτερο από το γινόμενο του κόστους της απώλειας επί την πιθανότητα να συμβεί αυτή τότε η υλοποίηση του μέτρου πρόληψης κρίνεται ως υπερβολική. Στην αντίθετη περίπτωση το μέτρο πρόληψης συμφέρει να υλοποιηθεί. Συνήθως τα μεγέθη υπολογίζονται σε ετήσιες απώλειες και ετήσια πιθανότητα να συμβεί ένα γεγονός. Η αντιστοίχηση των απωλειών

με οικονομικά νούμερα δεν είναι πάντα δυνατή διότι πολλές φορές στην ανάλυση των κινδύνων αξιολογούνται απώλειες απροσδιόριστες όπως η εικόνα ενός οργανισμού και η εμπιστοσύνη που έχουν οι «πελάτες» του σε αυτόν.

2.5 ΠΟΣΟΤΙΚΗ ΑΝΑΛΥΣΗ ΚΙΝΔΥΝΩΝ (Quantitative Risk Analysis)

Η ποσοτική εκτίμηση των κινδύνων αξιοποιεί τις μεθοδολογίες που χρησιμοποιούνται από οικονομολογικά ιδρύματα και ασφαλιστικές εταιρίες. Αναθέτοντας τιμές στις πληροφορίες, τα συστήματα, τις επιχειρηματικές διαδικασίες, το κόστος ανάκτησης κλπ., οι επιπτώσεις και επομένως ο κίνδυνος μπορούν να μετρηθούν από άποψη άμεσων και έμμεσων δαπανών.

Η ποσοτική ανάλυση προσπαθεί να προσδιορίσει αντικειμενικές αριθμητικές τιμές (πχ χρηματικά ποσά) για κάθε συνιστώσα της ανάλυσης κινδύνων. Για παράδειγμα προσπαθεί να υπολογίσει την χρηματική αξία των απωλειών ή την πιθανότητα να συμβεί ένα περιστατικό. Στην περίπτωση που ποσοτικοποιηθούν όλες οι συνιστώσες (αξία περιουσιακών στοιχείων, συχνότητα απειλών, αποτελεσματικότητα αντίμετρων, κόστος αντίμετρων, αβεβαιότητα και πιθανότητα) τότε η ανάλυση ονομάζεται πλήρως ποσοτική.

Μαθηματικά, ο ποσοτικός κίνδυνος μπορεί να εκφραστεί ως Ετησιοποιημένα Απώλεια Προσδόκιμου (Annualized Loss Expectancy (ALE)). ALE είναι η αναμενόμενη νομισματική ζημία που μπορεί να αναμένεται για ένα κεφάλαιο εξαιτίας του κινδύνου που πραγματοποιείται κατά τη διάρκεια ενός έτους.

ALE = SLE * ARO[2] , όπου SLE (Single Loss Expectancy – Ενιαίο Προσδόκιμο Απώλειας) και ARO (Annualized Rate of Occurrence - Ετησιοποιημένος Ρυθμός Εμφάνισης).

Από μαθηματικής άποψης, αυτό γίνεται περίπλοκο πολύ γρήγορα, με τη συμμετοχή στατιστικών τεχνικών. Ενώ η χρήση ποσοτικής εκτίμησης του κινδύνου φαίνεται απλή και λογική, υπάρχουν θέματα με τη χρήση της στα συστήματα πληροφοριών. Ενώ το κόστος ενός συστήματος μπορεί να είναι εύκολο να καθοριστεί, το έμμεσο κόστος, όπως η αξία των πληροφοριών, η χαμένη παραγωγική δραστηριότητα και το κόστος ανάκτησης είναι ατελώς γνωστή στην καλύτερη περίπτωση. Επιπλέον, το άλλο σημαντικό στοιχείο του κινδύνου, η πιθανότητα, είναι συχνά ακόμη λιγότερο απόλυτα γνωστή.

Ως εκ τούτου, ένα μεγάλο περιθώριο λάθους είναι συνήθως συνυφασμένο με την ποσοτική εκτίμηση του κινδύνου στα πληροφοριακά συστήματα. Αυτό μπορεί να μην συμβαίνει πάντα στο μέλλον. Δεδομένου ότι το σώμα των στατιστικών στοιχείων είναι διαθέσιμο, οι τάσεις μπορούν να επεκτείνουν την εμπειρία του παρελθόντος. Οι ασφαλιστικές εταιρίες και τα χρηματοοικονομικά ιδρύματα κάνουν άριστη χρήση αυτών των στατιστικών προκειμένου να εξασφαλίσουν ότι η ποσοτική αξιολόγηση του κινδύνου τους έχει νόημα, είναι επαναλαμβανόμενη και συνεπής. Τυπικά, δεν είναι οικονομικά αποδοτική για να εκτελέσει μία ποσοτική εκτίμηση του κινδύνου σε ένα πληροφοριακό σύστημα, λόγω της σχετικής δυσκολίας απόκτησης ακριβών και πλήρη πληροφοριών.

Ωστόσο, αν η πληροφορία θεωρείται αξιόπιστη, μία ποιοτική εκτίμηση κινδύνου αποτελεί ένα εξαιρετικά ισχυρό εργαλείο για την ανακοίνωση του κινδύνου σε όλα τα επίπεδα της διοίκησης. Η ποσοτική μέτρηση του κινδύνου είναι τυπική.

Συμπερασματικά, ποσοτική μέτρηση του κινδύνου είναι ο συνήθης τρόπος μέτρησης του κινδύνου σε πολλούς τομείς, όπως η ασφάλιση, αλλά δεν χρησιμοποιείται συνήθως για τη μέτρηση του κινδύνου σε πληροφοριακά συστήματα.
Δύο λόγοι που συμβαίνει αυτό είναι:

- Οι δυσκολίες στον προσδιορισμό και τη απόδοση αξίας των κεφαλαίων
- Η έλλειψη στατιστικών πληροφοριών που θα καθιστούσαν δυνατό τον προσδιορισμό της συχνότητας.

Έτσι, τα περισσότερα από τα εργαλεία που χρησιμοποιούνται σήμερα για την αξιολόγηση του κινδύνου είναι μετρήσεις του ποιοτικού κινδύνου.

2.6 ΠΟΙΟΤΙΚΗ ΑΝΑΛΥΣΗ ΚΙΝΔΥΝΩΝ (Qualitative Risk Analysis)

Η ποιοτική ανάλυση των κινδύνων είναι μία τεχνική κατά την οποία επιχειρείται να προσδιοριστεί το επίπεδο ασφάλειας που απαιτείται για ένα πληροφοριακό σύστημα. Αυτό επιτυγχάνεται με μία συστηματική εξέταση :

- Των περιουσιακών στοιχείων
- Των απειλών
- Των ευπαθειών
- Του κόστους των απωλειών σε περίπτωση που συμβούν
- Του κόστους των αντιμέτρων σε περίπτωση που μπορεί να χρησιμοποιηθούν για την μείωση των απειλών και ευπαθειών

Η ποιοτική ανάλυση επιχειρεί να δώσει προτεραιότητες στους διάφορους κινδύνους με υποκειμενικά κριτήρια και όχι να τους υπολογίσει ακριβώς.
Υπάρχουν πολλές διαφορετικές τεχνικές για ποιοτική ανάλυση κινδύνων. Η ποιοτική ανάλυση σε 10 βήματα είναι αντιπροσωπευτική για την κατηγορία της.

Βήμα 1^{ο} : καθορισμός του σκοπού της ανάλυσης

Πριν αρχίσει η ανάλυση πρέπει να καθοριστεί με ακρίβεια ο σκοπός και η εμβέλειά της. Πρέπει να περιγραφεί το πληροφοριακό σύστημα που θα εξεταστεί (πχ. ένα μηχανογραφικό κέντρο, ένα εταιρικό δίκτυο κλπ). Για να αποφευχθεί η ολίσθηση της ανάλυσης πρέπει να καθοριστούν με σαφή τρόπο τα όρια της. Η ανάλυση πρέπει να

επικεντρωθεί στα συστήματα που υπάρχει άμεσος τρόπος παρέμβασης. Για παράδειγμα αν μία εφαρμογή χρησιμοποιεί ένα ξένο δίκτυο (πχ. internet) για να ανταλλάσσει δεδομένα, δεν έχει νόημα η ανάλυση κινδύνων του δικτύου αυτού αφού ουσιαστικά δεν μπορούμε να παρέμβουμε σε αυτό. Στα πληροφοριακά συστήματα οι στόχοι της ανάλυσης κινδύνων έχουν να κάνουν με το αντίκτυπο που έχουν οι απειλές στην ακεραιότητα, εμπιστευτικότητα και διαθεσιμότητα των πληροφοριών. Είναι σημαντικό οι στόχοι της ανάλυσης να συνδέονται με την σωστή λειτουργία του οργανισμού και όχι με την ασφάλεια αυτή καθεαυτή. Η ασφάλεια υπάρχει για να υπηρετεί τον οργανισμό και όχι το αντίθετο.

Βήμα 2ο : δημιουργία ικανής ομάδας ανάλυσης κινδύνων

Ομάδα ανάλυσης κινδύνων είναι όλα τα άτομα που συμμετέχουν ενεργά στην διαδικασία της ανάλυσης κινδύνων. Επειδή η ποιοτική ανάλυση είναι μία υποκειμενική διαδικασία, η ποιότητα των αποτελεσμάτων εξαρτάται άμεσα από την εμπειρία και την ικανότητα των μελών της ομάδας που θα επιλεχθεί. Πολλοί ειδικοί ασφάλειας επιλέγουν να κάνουν την ανάλυση μόνοι τους ή σε συνεργασία με την ομάδα ασφάλειας του οργανισμού. Μία πιο αποτελεσματική διαδικασία ανάλυσης πρέπει να περιλαμβάνει στην ομάδα μέλη από όλες τις κατηγορίες χρηστών και διαχειριστών του πληροφοριακού συστήματος και άτομα με εξειδικευμένες γνώσεις (πχ. για φυσική ασφάλεια ή νομικές γνώσεις).
Ένα πολύ σημαντικό σημείο είναι η υποστήριξη και συμμετοχή στην διαδικασία της ανάλυσης κινδύνων τουλάχιστον ενός μέλους της διοίκησης (management) του οργανισμού. Αυτό βοηθά στην καλύτερη αποδοχή των αποτελεσμάτων της ανάλυσης. Εξασφαλίζοντας σωστή αντιπροσώπευση στην ομάδα ανάλυσης κινδύνων, τα αποτελέσματα που προκύπτουν έρχονται απευθείας από τους χρήστες και την διοίκηση και όχι σαν εξαναγκασμός από τους ειδικούς ασφάλειας.

Βήμα 3ο : αναγνώριση απειλών

Για κάθε περιουσιακό στοιχείο που εξετάζεται, η ομάδα ανάλυσης κινδύνων πρέπει να αναγνωρίσει τις διάφορες απειλές που μπορεί να προκαλέσουν απώλειες σε αυτό. Αυτό μπορεί να γίνει με πολλούς τρόπους. Ένας από αυτούς είναι να δοθεί στα μέλη της ομάδας μία λίστα με απειλές ώστε να επιλέξουν αυτές που νομίζουν ότι αντιστοιχούν στη συγκεκριμένη περίπτωση. Αυτό προϋποθέτει ο συντονιστής της ανάλυσης να έχει προετοιμάσει μία τέτοια λίστα από πριν ή να χρησιμοποιηθεί μία έτοιμη λίστα από μία γνωστική βάση (knowledge base). Ο τρόπος αυτός έχει το μεγάλο μειονέκτημα ότι τα μέλη της ομάδας συνήθως κοιτούν τη λίστα και δεν εκφράζουν τις δικές τους ιδέες. Αυτό μπορεί να αντιμετωπιστεί αν για έτοιμη λίστα πραγματοποιηθεί σύσκεψη για ανταλλαγή ιδεών (brainstorming). Αφού μαζευτούν όλες οι ιδέες μετά εγκρίνονται από το σύνολο

της ομάδας. Για την διευκόλυνση της διαδικασίας μπορεί να γίνει διερεύνηση των απειλών σε κατηγορίες. Για παράδειγμα μπορούν αρχικά να διερευνηθούν οι απειλές προς την ακεραιότητα, μετά προς την εμπιστευτικότητα κλπ. Το κλειδί για την επιτυχία είναι να ακουστούν όλες οι ιδέες και να κατηγοριοποιηθούν κατάλληλα.

Βήμα 4^{ο} : αξιολόγηση συχνότητας απειλών

Αφού τελειώσει το βήμα της αναγνώρισης των απειλών, η ομάδα ανάλυσης κινδύνων πρέπει να προσδιορίσει πόσο συχνά αναμένεται να συμβεί η κάθε μία από τις απειλές. Λόγω της ποιοτικής φύσης της ανάλυσης δεν χρειάζεται να υπολογιστεί η ακριβής συχνότητα της εμφάνισης των απειλών. Αρκεί απλά να προσδιοριστεί το πόσο συχνά ή σπάνια εντοπίζεται μία απειλή με βάση μία κλίμακα. Είναι απαραίτητο να καθοριστεί σαφώς τι σημαίνει η κάθε κατηγορία της κλίμακας ώστε όλα τα μέλη της ομάδας να επιλέγουν με βάση την ίδια έννοια. Υπάρχουν δύο τρόποι για τον καθορισμό της συχνότητας της κάθε απειλής. Ο πρώτος τρόπος είναι να επιλέξει το κάθε μέλος της ομάδας ξεχωριστά και μετά να βρεθεί ο μέσος όρος. Αφού γίνει αυτό, τα τελικά αποτελέσματα πρέπει να εγκριθούν από το σύνολο της ομάδας και να συζητηθούν οι περιπτώσεις όπου υπάρχουν επιλογές που απέχουν πολύ από τον μέσο όρο. Ο δεύτερος τρόπος είναι να μελετηθεί κάθε απειλή από το σύνολο της ομάδας με σκοπό την εύρεση κοινού αποτελέσματος.

Βήμα 5^{ο} : αξιολόγηση απειλών

Σε αυτό το βήμα η ομάδα ανάλυσης κινδύνων προσπαθεί να υπολογίσει τις απώλειες που μπορούν να προκύψουν σε περίπτωση που μία απειλή πραγματοποιηθεί. Οι ευπάθειες των περιουσιακών στοιχείων για κάθε απειλή σχετίζονται άμεσα με τις απώλειες που μπορούν να προκληθούν, οπότε πρέπει να ληφθούν σοβαρά υπόψη. Οι απώλειες υπολογίζονται για κάθε περιουσιακό στοιχείο και για κάθε απειλή που αντιστοιχεί σε αυτό. Για την πληρότητα και την ορθότητα της ανάλυσης η αξιολόγηση πρέπει να γίνει σαν να μην υπάρχει κανένα αντίμετρο εγκατεστημένο στο πληροφοριακό σύστημα. Η αποτελεσματικότητα των αντίμετρων που ήδη υπάρχουν εξετάζεται αργότερα. Η ομάδα καταλήγει σε αποτελέσματα είτε κάθε μέλος ξεχωριστά είτε όλοι μαζί.

Βήμα 6^{ο} : υπολογισμός δείκτη κινδύνου

Σε αυτό το βήμα η ομάδα προσθέτει τους αριθμούς της συχνότητας και της απώλειας και βρίσκει τον δείκτη κινδύνου, ο οποίος κυμαίνεται μεταξύ 2 και 10. Ο δείκτης κινδύνου προστίθεται στον πίνακα και ο πίνακας ταξινομείται με βάση αυτόν σε φθίνουσα σειρά. Επειδή κανένας οργανισμός δεν έχει τους πόρους να εξετάσει όλους τους κινδύνους, είναι

αναγκαίο να προσδιοριστεί ποιοι κίνδυνοι θα εξεταστούν περαιτέρω και σε τι βαθμό. Ο δείκτης κινδύνου, αν και προκύπτει υποκειμενικά, είναι ενδεικτικός για τις προτεραιότητες που πρέπει να δοθούν στην αντιμετώπιση των κινδύνων.

Βήμα 7^{ο} : αναγνώριση αντίμετρων

Αφού δοθούν προτεραιότητες στους διάφορους κινδύνους ακολουθεί το βήμα της αναγνώρισης των αντιμέτρων που μπορούν να τους αντιμετωπίσουν. Στο βήμα αυτό αναλύονται αρχικά οι ευπάθειες των περιουσιακών στοιχείων στις διάφορες απειλές και έπειτα γίνεται προσπάθεια εύρεσης των κατάλληλων αντιμέτρων που προσφέρουν αποδεκτό βαθμό προστασίας. Η ομάδα πρέπει να επικεντρώνει την προσοχή της σε αντίμετρα που αντιμετωπίζουν μεν τον κίνδυνο σε αποδεκτό βαθμό αλλά ταυτόχρονα επιτρέπουν και την σωστή λειτουργία του οργανισμού χωρίς να παρεμποδίζουν την παραγωγικότητα.
Τα αντίμετρα χωρίζονται σε 4 μεγάλες κατηγορίες:

- Πρόληψη : τα αντίμετρα αυτά προσπαθούν να μειώσουν τον κίνδυνο
- Διασφάλιση : εργαλεία, έλεγχοι και στρατηγικές που διασφαλίζουν την συνεχή αποτελεσματικότητα των παρόντων αντιμέτρων
- Ανίχνευση : προγράμματα και τεχνικές για έγκαιρη ανίχνευση, αναχαίτιση και αντιμετώπιση περιστατικών
- Επαναφορά : διαδικασίες που στοχεύουν στη γρήγορη επαναφορά σε ένα ασφαλές περιβάλλον έπειτα από ρήξη ασφαλείας και στην έρευνα της αιτίας που την προκάλεσε

Για την ευκολία της ομάδας μπορεί να χρησιμοποιηθεί λίστα με γνωστά αντίμετρα από τις 4 κατηγορίες. Ταυτόχρονα όμως πρέπει να λαμβάνονται υπόψη και οι απειλές που τυχόν χρειάζονται ειδικού τύπου αντίμετρα που δεν υπάρχουν σε λίστες. Αφού γίνει η επιλογή των πιθανών αντιμέτρων δημιουργείται ο πίνακας αναγνώρισης αντιμέτρων.

Βήμα 8^{ο} : ανάλυση κόστους / οφέλους (cost / benefit)

Κάθε αντίμετρο έχει κάποιο κόστος για τον οργανισμό. Το κόστος αυτό μπορεί να είναι χρηματικό, για την αγορά, εγκατάσταση και συντήρηση του αντιμέτρου. Μπορεί να είναι κόστος σε ανθρωποώρες για την ανάπτυξη διαδικασιών και πολιτικών ασφαλείας. Μπορεί επίσης να είναι κόστος από την παρεμπόδιση της κανονικής λειτουργίας του οργανισμού κατά την εγκατάσταση του αντίμετρου ή απώλειας παραγωγικότητάς λόγω της φύσης του. Σε όλες τις περιπτώσεις το κόστος πρέπει να λαμβάνεται υπόψη και να συγκρίνεται με το όφελος από την χρήση του αντιμέτρου. Λόγω της υποκείμενης φύσης της ποιοτικής ανάλυσης ίσως είναι αναγκαία η επανάληψη του υπολογισμού του δείκτη

κινδύνου, μόνο που αυτή τη φορά ο υπολογισμός γίνεται λαμβάνοντας υπόψη τα αντίμετρα που εξετάζονται. Έτσι μπορεί να αναλυθεί η αποτελεσματικότητά τους. Για να γίνει ένα αντίμετρο αποδεκτό πρέπει να μειώνει αποτελεσματικά τον κίνδυνο από μία ή περισσότερες απειλές. Η ανάλυση κόστους – οφέλους θα πρέπει να αναγνωρίσει τα αντίμετρα που προσφέρουν την μεγαλύτερη προστασία με το μικρότερο κόστος. Είναι σχεδόν πάντα προτιμότερο να επιλέγονται αντίμετρα που προστατεύουν περισσότερες από μία απειλές.

Βήμα 9^{ο} : ταξινόμηση αντιμέτρων με βάση την προτεραιότητα

Μετά το τέλος της ανάλυσης του κόστους – οφέλους η ομάδα ανάλυσης κινδύνων θα πρέπει να ταξινομεί τα αντίμετρα με βάση την προτεραιότητα για υλοποίηση. Επειδή οι πόροι που διαθέτονται για την ασφάλεια είναι περιορισμένοι, η διοίκηση του οργανισμού βασίζεται στην ομάδα ανάλυσης κινδύνων για την παροχή επαρκών πληροφοριών ώστε να προβεί σε σωστές αποφάσεις. Παράγοντες που επηρεάζουν τη σειρά προτεραιότητας είναι ο λόγος κόστους – οφέλους, ο αριθμός των απειλών που αντιμετωπίζει ένα αντίμετρο, το κατά πόσο μπορεί να υλοποιηθεί εσωτερικά στον οργανισμό ή χρειάζεται βοήθεια από εξωτερικούς παράγοντες. Είναι επιθυμητό να παρουσιάζονται οι λόγοι που οδήγησαν στην συγκεκριμένη επιλογή προτεραιοτήτων για τα αντίμετρα ώστε να γίνει κατανοητή από τη διοίκηση.

Βήμα 10^{ο} : έκθεση ανάλυσης κινδύνων

Τα αποτελέσματα της ανάλυσης κινδύνου πρέπει να παρουσιαστούν στην διοίκηση με μορφή έκθεσης. Η έκθεση αυτή υπηρετεί δύο σκοπούς : την αναφορά των αποτελεσμάτων και την ύπαρξη βάσης για τις μελλοντικές αναλύσεις κινδύνων. Μία έκθεση ανάλυσης κινδύνων θα μπορούσε να περιλαμβάνει τα εξής :

- Εισαγωγή
  Στην εισαγωγή περιγράφεται ο σκοπός της ανάλυσης κινδύνων και η εμβέλεια που αποφασίστηκε να έχει. Πρέπει να εξηγηθεί ποια συστήματα περιλήφθηκαν και γιατί. Επίσης μπορεί να αναφερθεί η μέθοδος που χρησιμοποιήθηκε καθώς και περιληπτικά τα βήματα που ακολουθήθηκαν.
- Αναγνώριση απειλών
  Περιγραφή των απειλών που αναγνωρίστηκαν καθώς και ο χειρισμός τους σε κατηγορίες. Μπορεί επίσης να αναφερθεί η διαδικασία που ακολουθήθηκε για την αναγνώριση των απειλών.
- Υπολογισμός δείκτη κινδύνου
  Αποτελέσματα από τον υπολογισμό του κινδύνου καθώς και επεξήγηση των παραγόντων που οδήγησαν σε αυτά (ευπάθειες, απώλειες, πιθανότητες). Αν

κατά τη διάρκεια της ανάλυσης υπήρχαν διαφωνίες μεταξύ των μελών της ομάδας, μπορούν να αναφερθούν σε αυτό το σημείο.

- Προτάσεις για αντίμετρα
  Το τελικό και πιο σημαντικό κομμάτι της έκθεσης είναι οι προτάσεις της ομάδας για την αντιμετώπιση των κινδύνων, δηλαδή τα προτεινόμενα αντίμετρα. Είναι επιθυμητό να αναφέρονται όλα τα αντίμετρα που αξιολογήθηκαν και η λογική με την οποία έγιναν οι συγκεκριμένες επιλογές. Επίσης σε ορισμένες περιπτώσεις μπορούν να δοθούν εναλλακτικά αντίμετρα ώστε να υπάρχει ευελιξία κατά το στάδιο της υλοποίησης της ασφάλειας. Σε περιπτώσεις που η ομάδα προτείνει την αποδοχή του κινδύνου για ορισμένες απειλές, πρέπει να εξηγεί επαρκώς την απόφαση αυτή. Τέλος η λίστα προτεραιότητας για την υλοποίησης των αντιμέτρων είναι πολύ σημαντική.

Κεφάλαιο 3 ΟΙΚΟΓΕΝΕΙΑ ISO 27000

Η σειρά των ISO/IEC 27000 (που είναι επίσης γνωστή ως 'ISMS Family of Standards' ή 'ISO 27k' για συντομία) περιλαμβάνει τα πρότυπα ασφάλειας πληροφοριών που εκδίδονται από τον διεθνή οργανισμό πιστοποίησης (ISO) και την International Electrotechnical Commission (IEC).
Η σειρά παρέχει τις καλύτερες συστάσεις πάνω στη διαχείριση της ασφάλειας πληροφοριών, τους κινδύνους και τους ελέγχους που πραγματοποιούνται για τα Information Security Management System (ISMS), παρόμοια στο σχεδιασμό με τα συστήματα διαχείρισης για τη διασφάλιση της ποιότητας (σειρά ISO 9000) και την προστασία του περιβάλλοντος (το ISO 14000 series) ..
Στην πραγματικότητα αυτά τα πρότυπα καλύπτουν πολλά περισσότερα από την εμπιστευτικότητα και τεχνικά θέματα ασφάλειας. Όλοι οι οργανισμοί ενθαρρύνονται να εκτιμήσουν τους κινδύνους της ασφάλειας πληροφοριών, έπειτα να εφαρμόσουν τους κατάλληλους ελέγχους ασφάλειας πληροφοριών σύμφωνα με τις ανάγκες τους, χρησιμοποιώντας καθοδήγηση και συστάσεις όπου κρίνεται απαραίτητο.
Τα πρότυπα εφαρμόζονται σε οργανισμούς κάθε είδους και μεγέθους. Προς το παρόν , είκοσι τρία από τα πρότυπα της σειράς δημοσιεύονται και είναι διαθέσιμα , ενώ πολλά άλλα βρίσκονται ακόμα υπό ανάπτυξη . Τα αρχικά πρότυπα ISO / IEC πωλούνται απευθείας από τον ISO , ενώ οι πωλήσεις των καταστημάτων συνδέονται με διάφορους εθνικούς φορείς τυποποίησης και πωλούν διάφορες εκδόσεις , συμπεριλαμβάνοντας τοπικές μεταφράσεις .

3.1 ISO/IEC 27005:2011

Information technology – security techniques – information security risk management

Ο σκοπός του ISO 27005 είναι να δώσει κατευθύνσεις για την Διαχείριση Κινδύνων Ασφάλειας Πληροφοριών. Το ISO 27005 υποστηρίζει τις γενικές έννοιες που ορίζονται στο πρότυπο ISO 27001 και έχει σχεδιαστεί για να βοηθήσει την ικανοποιητική εφαρμογή της Ασφάλειας Πληροφοριών βασίζεται σε μια προσέγγιση διαχείρισης κινδύνου. Το ISO 27005 δεν διευκρινίζει ούτε συνιστά οποιαδήποτε εξειδικευμένη μέθοδος ανάλυσης κινδύνου, αν και δεν προσδιορίζει μια δομημένη, συστηματική και αυστηρή διαδικασία από την ανάλυση των κινδύνων για τη δημιουργία του σχεδίου αντιμετώπισης του κινδύνου.
Το ISO/IEC 27005:2011 έχει τα εξής βήματα :

1. Εγκατάσταση πλαισίου (context establishment)
2. Αξιολόγηση κινδύνου (risk assessment)
3. Αντιμετώπιση κινδύνου (risk treatment)
4. Αποδοχή κινδύνου (risk acceptance)
5. Κοινοποίηση κινδύνου (risk communication)
6. Παρακολούθηση και επανεξέταση κινδύνου (risk monitoring and review).

Η εγκατάσταση πλαισίου είναι το 1^{ο} βήμα του πλαισίου ISO/IEC 27005. Σε αυτό περιλαμβάνεται η απόκτηση όλων των σχετικών πληροφοριών για την οργάνωση και τον καθορισμό των βασικών κριτηρίων, τον σκοπό, το πεδίο εφαρμογής, τα όρια και την οργάνωση των δραστηριοτήτων για τη διαχείριση κινδύνου.
Σκοπός, συνήθως, είναι η συμμόρφωση με τις νομικές απαιτήσεις και η παροχή αποδείξεων επιμέλειας που υποστηρίζει το ISMS που μπορεί να πιστοποιηθεί.
Το πεδίο εφαρμογής μπορεί να είναι ένα σχέδιο αναφοράς, ένα σχέδιο επιχειρησιακής συνέχειας ή η πιστοποίηση ενός προϊόντος.
Τα κριτήρια περιλαμβάνουν την εκτίμηση και αποδοχή του κινδύνου και τα κριτήρια αξιολόγησης των επιπτώσεων. Επίσης, προσδιορίζουν το πεδίο εφαρμογής και τα όρια του πλαισίου στον οργανισμό. Οι περιορισμοί του οργανισμού (δημοσιονομικοί, πολιτικοί, πολιτιστικοί, τεχνικοί) συλλέγονται και τεκμηριώνονται για να χρησιμοποιηθούν ως οδηγοί στα επόμενα βήματα.
Η αξιολόγηση κινδύνου λαμβάνει σαν είσοδο, την έξοδο του προηγούμενου βήματος, δηλαδή της εγκατάστασης πλαισίου. Η έξοδος είναι η λίστα των εκτιμώμενων κινδύνων κατά προτεραιότητα, σύμφωνα με τα κριτήρια αξιολόγησης των κινδύνων. Αυτή η διαδικασία μπορεί να χωριστεί σε:

1. Ανάλυση κινδύνου (risk analysis)
    a. Αναγνώριση κινδύνου (risk identification)
    b. Εκτίμηση κινδύνου (risk estimation)
2. Εκτίμηση κινδύνου (risk evaluation).

Ο κώδικας εφαρμογής του ISO/IEC 27002:2005 για τη διαχείριση ασφάλειας πληροφοριών συνιστά να εξεταστούν κατά τη διάρκεια της εκτίμησης του κινδύνου:

1. Η πολιτική ασφαλείας (διοικητική καθοδήγηση)
2. Η οργάνωση της ασφάλειας των πληροφοριών
3. Η διαχείριση περιουσιακών στοιχείων (ταξινόμηση των πληροφοριακών αγαθών)
4. Η φυσική και περιβαλλοντική ασφάλεια
5. Η διαχείριση επικοινωνιών και λειτουργιών
6. Ο έλεγχος πρόσβασης (περιορισμός των δικαιωμάτων πρόσβασης σε δίκτυα, συστήματα, εφαρμογές και δεδομένα)

7. Η απόκτηση, η ανάπτυξη και η συντήρηση πληροφοριακού συστήματος
8. Η διαχείριση περιστατικών της ασφάλειας πληροφοριών
9. Η διαχείριση επιχειρησιακής συνέχειας (προστασία, συντήρηση και ανάρρωση των ευαίσθητων επιχειρηματικών διαδικασιών και συστημάτων)
10. Η συμμόρφωση (διασφάλιση της συμμόρφωσης με τις πολιτικές ασφαλείας, τα πρότυπα, το νόμο και τους κανονισμούς).

Η αναγνώριση των κινδύνων αναφέρει τι θα μπορούσε να προκαλέσει μία πιθανή απώλεια.
Έτσι, πρέπει να προσδιορίζονται :

1. Τα περιουσιακά στοιχεία
    a. Πρωτογενή (δηλαδή επιχειρηματικές διεργασίες και σχετικές πληροφορίες)
    b. Υποστήριξη (hardware, software, προσωπικό, τοποθεσία, οργανωτική δομή)
2. Οι απειλές
3. Τα μέτρα ασφαλείας
4. Οι ευπάθειες
5. Οι συνέπειες
6. Οι σχετιζόμενες επιχειρηματικές διαδικασίες

Η έξοδος των επιμέρους διεργασιών αποτελείται από έναν κατάλογο με τα περιουσιακά στοιχεία και τις σχετιζόμενες επιχειρηματικές διαδικασίες που διαχειρίζεται τον κίνδυνο με τον σχετικό κατάλογο απειλών και μέτρων ασφαλείας. Επιπλέον, έχει έναν κατάλογο με τις ευπάθειες που δεν σχετίζονται με τις προσδιορισμένες απειλές και έναν κατάλογο με περιστατικά σεναρίων και τις συνέπειές τους.

Η εκτίμηση κινδύνου έχει ως είσοδο, την έξοδο της ανάλυσης του κινδύνου και χωρίζεται στα εξής βήματα :

1. Εκτίμηση των συνεπειών μέσω της αποτίμησης των περιουσιακών στοιχείων
2. Εκτίμηση της πιθανότητας του περιστατικού μέσω των απειλών και την αποτίμησης της ευπάθειας
3. Εκχώρηση τιμών στην πιθανότητα και την συνέπεια των κινδύνων.

Η έξοδος είναι η λίστα των κινδύνων με τα επίπεδα αξίας που έχουν ανατεθεί και τεκμηριώνεται σε ένα μητρώο κινδύνου.

Η διαδικασία αξιολόγησης του κινδύνου λαμβάνει ως είσοδο, την έξοδο της διαδικασίας ανάλυσης κινδύνου. Συγκρίνει κάθε επίπεδο με βάση τα κριτήρια αποδοχής και την προτεραιότητα στη λίστα αντιμετώπισης του κινδύνου.

Η μείωση κινδύνου είναι η τρίτη διαδικασία σύμφωνα με το πρότυπο ISO 27005. Περιλαμβάνει την ιεράρχηση, την αξιολόγηση και την εφαρμογή των κατάλληλων ελέγχων για τη μείωση του κινδύνου, που συνιστάται από την διαδικασία εκτίμησης κινδύνου.
Η διαδικασία αντιμετώπισης του κινδύνου αποσκοπεί στην επιλογή των μέτρων ασφαλείας για την μείωση, τη διατήρηση, την αποφυγή και τη μεταφορά του κινδύνου καθώς και στην παραγωγή ενός σχεδίου αντιμετώπισής του.
Η έξοδος της διαδικασίας είναι το σχέδιο αντιμετώπισης με τους εναπομένοντες κινδύνους που συνδέονται με την αποδοχή της διαχείρισης.

Η κοινοποίηση των κινδύνων είναι μία διαδικασία που αλληλεπιδρά αμφίδρομα με όλες τις διαδικασίες της διαχείρισης των κινδύνων. Σκοπός της είναι η ύπαρξη μιας κοινής αντίληψης για όλες τις πτυχές του κινδύνου μεταξύ των ενδιαφερόμενων μερών του οργανισμού.

Η διαχείριση των κινδύνων είναι μία συνεχή και ατέρμονη διαδικασία. Στο πλαίσιο αυτής της διαδικασίας εφαρμόζονται τα μέτρα ασφάλειας, τα οποία παρακολουθούνται τακτικά και αξιολογούνται ώστε να εξασφαλιστεί ότι λειτουργούν σύμφωνα με το πρόγραμμα. Όμως, οι απαιτήσεις, οι ευπάθειες και οι απειλές μπορούν να αλλάξουν με την πάροδο του χρόνου. Γι' αυτό πρέπει να προγραμματίζονται τακτικοί έλεγχοι και να διεξάγονται από κάποιο ανεξάρτητο άτομο, δηλαδή από κάποιον που δεν είναι υπεύθυνος για τις εφαρμογές ή την καθημερινή διαχείριση ISMS.

3.2 ISO/IEC 27001

Το ISO/IEC 27001 είναι μέρος μίας αναπτυσσόμενης οικογένειας των ISO/IEC standards ('ISO/IEC 27000 series') είναι ένα πρότυπο σύστημα διαχείρισης ασφάλειας πληροφοριών (ISMS) το οποίο εκδόθηκε τον Οκτώβρη του 2005 από τον διεθνή οργανισμό πιστοποίησης (ISO) και την International Electrotechnical Commission (IEC). Το πλήρες του όνομα είναι ISO/IEC 27001 :2005 – Information technology – Security techniques – Information security management systems – requirements αλλά για λόγους συντομίας αναφερόμαστε σε αυτό με το "ISO 27001".
Πρόκειται να χρησιμοποιηθεί σε συνδυασμό με το ISO/IEC 27002, the Code of Practice for Information Security Management, το οποίο βρίσκεται στην λίστα των σκοπών ελέγχου ασφαλείας και συνιστά ένα εύρος συγκεκριμένων ελέγχων ασφαλείας. Οι οργανισμοί οι οποίο θα εφαρμόσουν ένα ISMS σύμφωνα με την καλύτερη πρακτική συμβουλή στο ISO/IEC 27002 είναι πιθανότατα ταυτόχρονα καλυμμένοι για τις

απαιτήσεις του ISO/IEC 27001 αλλά η επικύρωση με το δίπλωμα είναι καθαρά προαιρετική.

Το ISO/IEC 27001:2005 υιοθετεί το πρότυπο της διαδικασίας "Plan – Do – Check – Act" (PDCA), το οποίο εφαρμόζεται στη δομή όλων των διαδικασιών ενός ISMS.

- Plan (καθορισμός του ISMS)
  Καθιέρωση της πολιτικής, των στόχων του ISMS, των διεργασιών και διαδικασιών που σχετίζονται με τη διαχείριση των κινδύνων, και βελτίωση της ασφάλειας των πληροφοριών ώστε να παρέχονται αποτελέσματα σύμφωνα με τις παγκόσμιες πολιτικές και τους στόχους της οργάνωσης.

- Do (εφαρμογή και λειτουργία του ISMS)
  Εφαρμογή και εκμετάλλευση της πολιτικής ISMS, των ελέγχων και των διαδικασιών.

- Check (παρακολούθηση και επανεξέταση του ISMS)
  Αξιολόγηση και μέτρηση των επιδόσεων των διαδικασιών ενάντια στην πολιτική, στους στόχους, στην πρακτική εμπειρία και την έκθεση των αποτελεσμάτων της διαχείρισης για επανεξέταση.

- Act (αναβάθμιση και βελτίωση του ISMS)
  Γίνονται διορθωτικές και προληπτικές ενέργειες με βάση τα αποτελέσματα του εσωτερικού ελέγχου του ISMS και της επανεξέτασης της διαχείρισης ή άλλων σχετικών πληροφοριών ώστε να επιτυγχάνεται η συνεχή βελτίωση του συστήματος.

Οι τομείς του ISO/IEC 27001:2005 είναι:

- Διαχείριση περιουσιακών στοιχείων (asset management)
- Εγγραφή περιουσιακών στοιχείων (asset register)
- Ταξινόμηση περιουσιακών στοιχείων (asset classification)
- Σήμανση περιουσιακών στοιχείων (asset labeling)
- Έλεγχος πρόσβασης (access control)
- Εγγραφή χρήστη (user registration)
- Διαχείριση κωδικών πρόσβασης (password management)
- Καθαρισμός εργασιακού περιβάλλοντος (clear work environment)

- Λειτουργικό σύστημα και έλεγχος εφαρμογής (operating system and application control)
- Ασφάλεια δικτύου (network security).

Η πιστοποίηση με το πρότυπο ISO/IEC 27001, συνήθως εμπεριέχει μία διαδικασία με τρία βήματα:

- Στο πρώτο βήμα γίνεται μία ανασκόπηση της ύπαρξης και της πληρότητας σημαντικών εγγράφων όπως η πολιτική ασφαλείας του οργανισμού, Statement of Applicability (SoA) and Risk Treatment Plan (RTP).

- Στο δεύτερο βήμα γίνεται ένας λεπτομερής σε βάθος έλεγχος για την ύπαρξη και την αποτελεσματικότητα των ελέγχων ασφάλειας που δηλώνονται στο SoA και στο RTP καθώς επίσης και τα υποστηρικτικά τους έγγραφα.

- Στο τρίτο βήμα πραγματοποιείται μία επανεκτίμηση για να επιβεβαιώσει ότι ο οργανισμός ο οποίος έχει ήδη πιστοποιηθεί, παραμένει συμμορφωμένος με το πρότυπο. Η συντήρηση της πιστοποίησης περιέχει περιοδικές ανασκοπήσεις και επανεκτιμήσεις για να επιβεβαιωθεί ότι το ISMS συνεχίζει να λειτουργεί όπως έχει καθοριστεί.

Το ISO/IEC 27001:2005 αντικαταστήθηκε από το νέο πρότυπο ISO/IEC 27001:2013, το οποίο δίνει μεγαλύτερη έκφραση στη μέτρηση και την αξιολόγηση της καλής λειτουργίας του οργανισμού και υπάρχει ένα επιπλέον κεφάλαιο για την εξωτερική ανάθεση, όπου αντανακλά το γεγονός ότι πολλοί οργανισμοί βασίζονται σε τρίτα μέρη ώστε να παρέχουν ορισμένες πτυχές της πληροφορικής. Επιπλέον δεν τονίζεται ο κύκλος "Plan – Do – Check – Act" όπως στο προηγούμενο και πρέπει να καταβάλλεται περισσότερη προσοχή στο οργανωτικό πλαίσιο της ασφάλειας των πληροφοριών, καθώς άλλαξε η εκτίμηση του κινδύνου.

Κεφάλαιο 4 ΒΑΣΙΚΕΣ ΜΕΘΟΔΟΛΟΓΙΕΣ ΓΙΑ ΤΗΝ ΑΞΙΟΛΟΓΗΣΗ ΚΑΙ ΤΗ ΔΙΑΧΕΙΡΙΣΗ ΤΗΣ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ ΣΤΑ ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ

4.1 Μέθοδος CRAMM

Η μέθοδος CRAMM (CCTA Risk Analysis and Management Methodology) αναπτύχθηκε από την Κεντρική Υπηρεσία Υπολογιστών και Τηλεπικοινωνιών (Central Computer and Telecommunications Agency – CCTA)του Ηνωμένου Βασιλείου το 1987 και αποτελεί πρότυπο για τους οργανισμούς του ευρύτερου δημόσιου τομέα στο Ηνωμένο Βασίλειο. Η CRAMM έχει κερδίσει διεθνή αναγνώριση για τους εξής λόγους:

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

Το λογισμικό υποστήριξης της CRAMM υποστηρίζει το σύνολο της μεθόδου και αποτελεί αναπόσπαστο τμήμα της. Μέσω του εργαλείου αυτού παρακολουθείται η ορθή εφαρμογή της μεθοδολογίας Ανάλυσης και Διαχείρισης Επικινδυνότητας, ενώ αποθηκεύονται και ενημερώνονται όλα τα στοιχεία που συλλέγονται κατά την εφαρμογή της μεθοδολογίας. Επίσης, το εργαλείο CRAMM υποστηρίζει όλους τους σύνθετους υπολογισμούς που απαιτούνται για τον προσδιορισμό της επικινδυνότητας, ενσωματώνει την βάση των αντιμέτρων και τους μηχανισμούς συμπερασματολογίας που προτείνουν τα αντίμετρα.

Η CRAMM αποτελείται από τρία βασικά στάδια:

1. Προσδιορισμός – αξιολόγηση των αγαθών (identification and valuation of assets)
2. Ανάλυση επικινδυνότητας (risk analysis)
3. Διαχείριση επικινδυνότητας (risk management)

1. <u>Προσδιορισμός – αξιολόγηση των αγαθών</u>

Το πρώτο στάδιο αναφέρεται στον προσδιορισμό και την αξιολόγηση των στοιχείων των πληροφοριακών συστημάτων που χρειάζονται προστασία. Αποτελείται από τα εξής βήματα:

- Δημιουργία συνοπτικού μοντέλου των πληροφοριακών συστημάτων
- Αποτίμηση των στοιχείων των πληροφοριακών συστημάτων
- Επιβεβαίωση και επικύρωση της αποτίμησης

1.1. Δημιουργία μοντέλου πληροφοριακού συστήματος

Το πρώτο βήμα αναφέρεται στον προσδιορισμό των στοιχείων των πληροφοριακών συστημάτων που απαιτούν προστασία. Τα στοιχεία αυτά είναι τα δεδομένα που χειρίζονται, όπως επίσης το λογισμικό και το υλικό των πληροφοριακών συστημάτων. Τα στοιχεία αυτά βρίσκονται σε αλληλεπίδραση.
Η συλλογή των απαραίτητων στοιχείων βασίζεται στην τεκμηρίωση του συστήματος και στον πρώτο κύκλο συνεντεύξεων που αφορά το τεχνικό προσωπικό και τους κύριους χρήστες του πληροφοριακού συστήματος. Αυτές οι κατηγορίες προσωπικού μπορούν να προσφέρουν πλήρη εικόνα για την λειτουργικότητα των πληροφοριακών συστημάτων του οργανισμού. Το μοντέλο του συστήματος εισάγεται στο εργαλείο λογισμικού της CRAMM και ελέγχεται η συνέπεια του.

1.2. Αποτίμηση αγαθών

Κατά την αποτίμηση των στοιχείων των πληροφοριακών συστημάτων, δίνεται ιδιαίτερη έμφαση στην αποτίμηση των δεδομένων που διαχειρίζεται προκειμένου να προσδιοριστεί η σπουδαιότητα που έχουν αυτά για την υπηρεσία. Η αξία κάθε ομάδας / κατηγορίας δεδομένων αποτιμάται με βάση την επίπτωση (impact) που θα είχε η απώλεια της. Εξετάζεται το μέγεθος της επίπτωσης στις περιπτώσεις καταστροφής, μη εξουσιοδοτημένης μεταβολής (modification), αποκάλυψης (disclosure) και μη διαθεσιμότητας (unavailability).
Συγκεκριμένα εξετάζονται οι εξής περιπτώσεις:

- Μη διαθεσιμότητα
- Καταστροφή (απώλεια των δεδομένων μετά τη λήψη του τελευταίου αντιγράφου ασφαλείας)
- Αποκάλυψη (αποκάλυψη των δεδομένων σε μη εξουσιοδοτημένα άτομα)
- Μη εξουσιοδοτημένη μεταβολή (μικρής και μεγάλης έκτασης σφάλματα)
- Εκούσια μεταβολή δεδομένων
- Σφάλματα μετάδοσης δεδομένων

Για κάθε περίπτωση εκτιμάται το δυσμενέστερο πιθανό σενάριο και υπολογίζονται οι επιπτώσεις από την πραγματοποίηση του. Το μέγεθος της επίπτωσης υπολογίζεται αριθμητικά με κλίμακα 1 – 10. Η CRAMM παρέχει οδηγίες (guidelines) για την αποτίμηση των επιπτώσεων που ανήκουν στις παρακάτω κατηγορίες:

- Επιπτώσεις στη σωματική ακεραιότητα και τη ζωή φυσικών προσώπων
- Επιπτώσεις από την αποκάλυψη ευαίσθητων προσωπικών δεδομένων
- Νομικές επιπτώσεις
- Παρεμπόδιση εφαρμογής της δικαιοσύνης και της εξιχνίασης παρανομιών
- Οικονομικές απώλειες
- Διατάραξη της δημόσιας τάξης
- Διεθνείς σχέσεις
- Άμυνα και εθνική ασφάλεια
- Εφαρμογή της πολιτικής του οργανισμού
- Απώλεια της εμπιστοσύνης του κοινού στον οργανισμό.

Ακολούθως η CRAMM μέσω του αυτοποιημένου εργαλείου υπολογίζει την έμμεση αξία (implied value) των στοιχείων των πληροφοριακών συστημάτων.
Η αποτίμηση των πληροφοριακών συστημάτων βασίζεται σε συνεντεύξεις που γίνονται με στελέχη που εμπλέκονται στην αξιοποίηση του πληροφοριακού συστήματος.
Το λογισμικό της CRAMM αποθηκεύει και επεξεργάζεται τα δεδομένα που συλλέγονται και πραγματοποιεί το συσχετισμό της αποτίμησης των επιμέρους στοιχείων του συστήματος με το μοντέλο του συστήματος. Έτσι υπολογίζεται η έμμεση αξία των στοιχείων του συστήματος.

1.3. Επιβεβαίωση και επικύρωσης της αποτίμησης

Η αποτίμηση των αγαθών των πληροφοριακών συστημάτων αποτελεί κρίσιμο παράγοντα για τη συνέχεια της μελέτης ανάλυσης και διαχείρισης επικινδυνότητας. Το κύριο προϊόν αυτού του σταδίου είναι η αποτίμηση των αγαθών. Τα αποτελέσματα του πρώτου σταδίου παρουσιάζονται σε σχετική έκθεση η οποία περιλαμβάνει:

- Τον ορισμό του προς ανάλυση συστήματος και των ορίων του
- Τη μέθοδο εργασίας που ακολουθήθηκε
- Την αποτίμηση των περιουσιακών στοιχείων των πληροφοριακών συστημάτων
- Γενικά συμπεράσματα του πρώτου σταδίου

2. Ανάλυση επικινδυνότητας (risk analysis)

Στο πρώτο στάδιο υπολογίστηκε ένας από τους τρεις παράγοντες που συνθέτουν την επικινδυνότητα. Συγκεκριμένα, αποτιμήθηκε η αξία των στοιχείων των πληροφοριακών συστημάτων τα οποία εφόσον έχουν αξία θα ονομάζονται αγαθά ή περιουσιακά στοιχεία. Στο δεύτερο στάδιο υπολογίζονται οι άλλοι δύο παράγοντες, το επίπεδο των απειλών (threat level) και το επίπεδο των αδυναμιών του συστήματος (vulnerability level). Ο συνδυασμός των τριών παραγόντων δίδει το βαθμό επικινδυνότητας του συστήματος, έτσι ώστε να επιλεγούν τα κατάλληλα αντίμετρα. Τα βήματα που ακολουθούνται είναι τα εξής:

- Προσδιορισμός των απειλών που αφορούν το κάθε αγαθό
- Εκτίμηση απειλών και αδυναμιών
- Υπολογισμός της επικινδυνότητας για κάθε συνδυασμό αγαθό – απειλή – αδυναμία
- Επιβεβαίωση και επικύρωση του βαθμού επικινδυνότητας

2.1. Προσδιορισμός των απειλών που αφορούν κάθε αγαθό

Η μέθοδος CRAMM δεν περιορίζεται στον υπολογισμό των πιθανών απειλών που υφίσταται ένα πληροφοριακό σύστημα, αλλά επικεντρώνεται στον προσδιορισμό συγκεκριμένων απειλών για κάθε αγαθό. Η CRAMM παρέχει μία ενδεικτική λίστα απειλών, καθώς και συστάσεις για το ποιες κατηγορίες στοιχείων ενός πληροφοριακού συστήματος αντιμετωπίζουν συνήθως τη συγκεκριμένη απειλή. Όταν ένα από τα στοιχεία των πληροφοριακών συστημάτων αντιμετωπίζει απειλή τότε και τα δεδομένα ή οι υπηρεσίες που υποστηρίζει αντιμετωπίζουν την ίδια απειλή. Με την CRAMM ο αναλυτής δεν χρειάζεται να υπολογίζει ο ίδιος τις συσχετίσεις και αλληλεπιδράσεις.
Το CRAMM – εργαλείο ζητά από τους αναλυτές να συσχετίσουν τα αγαθά με κατηγορίες απειλών από την κατάσταση. Έτσι, το εργαλείο προβαίνει σε συμπεράσματα με βάση το μοντέλο του συστήματος. Για παράδειγμα, αν μία απειλή συσχετισθεί με μία τοποθεσία, τότε το εργαλείο συμπεραίνει ότι η απειλή αυτή αφορά το σύνολο των αγαθών που βρίσκονται στη συγκεκριμένη τοποθεσία.

2.2. Εκτίμηση απειλών και αδυναμιών

Για κάθε συνδυασμό αγαθού – απειλής εκτιμάται το μέγεθος της απειλής και η σοβαρότητα των αδυναμιών που μπορεί να οδηγήσουν στην πραγματοποίηση της απειλής. Η CRAMM υπολογίζει το επίπεδο της απειλής με βάση απαντήσεις σε ερωτηματολόγια των απειλών. Η εκτίμηση της απειλής γίνεται σε κλίμακα από 1-5.

Αντίστοιχα, για τις αδυναμίες συμπληρώνονται ερωτηματολόγια και υπολογίζεται η σοβαρότητα της αδυναμίας σε κλίμακα 1-3.

Το εργαλείο της CRAMM παρέχει ερωτηματολόγια για κάθε συνδυασμό απειλής – αγαθού. Οι απαντήσεις εισάγονται στο λογισμικό της CRAMM και υπολογίζεται το επίπεδο των απειλών και των αδυναμιών. Επίσης, παρέχεται η δυνατότητα στους αναλυτές να αλλάξουν τις τιμές που υπολογίστηκαν αυτοματοποιημένα. Προκύπτει μία αναφορά για την εκτίμηση των απειλών - αδυναμιών ώστε να αξιολογηθούν τα αποτελέσματα αυτής της διαδικασίας.

2.3. Υπολογισμός επικινδυνότητας για κάθε συνδυασμό αγαθό – απειλή – αδυναμία

Η CRAMM υπολογίζει για κάθε συνδυασμό αγαθό – απειλή – αδυναμία το βαθμό επικινδυνότητας. Για το σκοπό αυτό, χρησιμοποιούνται τόσο τα αποτελέσματα της εκτίμησης απειλών και αδυναμιών όσο και το μοντέλο των πληροφοριακών συστημάτων. Ο υπολογισμός του βαθμού επικινδυνότητας ακολουθεί μία κλίμακα 1-7 και γίνεται αυτόματα για κάθε συνδυασμό αγαθού – απειλής – αδυναμίας. Ο αναλυτής έχει τη δυνατότητα να παρέμβει και να αλλάξει κάποιες τιμές αν το θεωρεί σκόπιμο.

2.4. Επικύρωση του βαθμού επικινδυνότητας

Η ομάδα μελέτης μπορεί να χρησιμοποιήσει τις αναφορές που παράγει το λογισμικό της CRAMM και το εργαλείο back-track για να εξετάσει συνολικά το βαθμό επικινδυνότητας. Σε περίπτωση που κριθεί ότι χρειάζεται να γίνουν κάποιες αλλαγές, τότε οι αναλυτές είτε αλλάζουν τις τιμές επικινδυνότητας είτε αλλάζουν τις τιμές που έχουν προκύψει από την εκτίμηση των απειλών και αδυναμιών και υπολογίζουν εκ νέου την επικινδυνότητα.

3. Διαχείριση επικινδυνότητας

Η μέθοδος CRAMM παράγει ένα σχέδιο ασφάλειας για τα πληροφορικά συστήματα με βάση τα αποτελέσματα του 2^{ου} σταδίου. Αυτό αποτελείται από μία σειρά αντιμέτρων τα οποία κρίνονται απαραίτητα για την αντιμετώπιση και διαχείριση της επικινδυνότητας και τα οποία θα πρέπει να εφαρμοστούν. Το σχέδιο ασφάλειας περιλαμβάνει μία σειρά επιλογών και εναλλακτικών λύσεων ώστε να παρέχεται ευελιξία στην εφαρμογή του.

Για τα συστήματα που έχουν ήδη αναπτυχθεί και λειτουργούν το προτεινόμενο σχέδιο ασφάλειας μπορεί να συγκριθεί με τα υπάρχοντα αντίμετρα. Η τελική επιλογή λαμβάνει υπόψη και το κόστος που έχουν τα αντίμετρα στον οργανισμό.

3.1. Προσδιορισμός των προτεινόμενων αντιμέτρων

Η CRAMM περιλαμβάνει μία ευρεία βάση αντιμέτρων.
Τα αντίμετρα αυτά είναι τεχνικά, διοικητικά και οργανωτικά. Το λογισμικό της CRAMM μπορεί να επιλέξει αυτόματα μία κατάσταση προτεινόμενων αντιμέτρων με βάση τα αποτελέσματα της ανάλυσης επικινδυνότητας. Τα αντίμετρα χωρίζονται σε ομάδες, ανάλογα με το είδος των απειλών που καλούνται να αντιμετωπίσουν και ανάλογα με το είδος των αγαθών που καλούνται να προστατέψουν. Η βάση των αντιμέτρων περιλαμβάνει τόσο τις εναλλακτικές λύσεις, δηλαδή ποιο αντίμετρο μπορεί να χρησιμοποιηθεί εναλλακτικά άλλου, καθώς και επιλογές υλοποίησής τους. Μεταξύ των προτεινόμενων αντίμετρων πρέπει να γίνουν συγκεκριμένες επιλογές. Οι επιλογές αυτές βασίζονται σε πολύ σημαντικό βαθμό στην εμπειρία των αναλυτών. Η CRAMM βοηθά, ώστε οι επιλογές να ακολουθούν μία δομημένη προσέγγιση και να αιτιολογούνται επαρκώς. Τα κριτήρια που λαμβάνονται υπόψη στην τελική επιλογή περιλαμβάνουν τα εξής:

- Την επίδραση που θα έχουν τα αντίμετρα στη λειτουργία του οργανισμού.
- Τον υπάρχοντα προϋπολογισμό για την ασφάλεια των πληροφοριακών συστημάτων.
- Το κόστος εγκατάστασης και λειτουργίας των αντιμέτρων.
- Την άποψη της διοίκησης και τους στόχους της.
- Ενδεχόμενες ενδείξεις ότι οι απειλές θα αυξηθούν στο μέλλον.

Ακολούθως τα προτεινόμενα αντίμετρα συγκρίνονται με τα υπάρχοντα. Το λογισμικό της CRAMM περιέχει μία βάση με περισσότερα από 2.500 αντίμετρα, ενταγμένα σε ομάδες και ιεραρχημένα ανάλογα με το επίπεδο ασφάλειας που προσφέρουν. Το CRAMM εργαλείο επιλέγει αυτόματα τα αντίμετρα σύμφωνα με τα αποτελέσματα της ανάλυσης επικινδυνότητας. Η κατάσταση-απόφαση για ένα αντίμετρο μπορεί να είναι:

- Εγκατεστημένο (installed)
- Προς υλοποίηση (to be installed)
- Υπό υλοποίηση (implementing recommendation)
- Προτεινόμενο για υλοποίηση (implemented recommendation)
- Έχει καλυφθεί ήδη (already covered)
- Αναλαμβάνεται η επικινδυνότητα (accept level of risk)
- Υπό συζήτηση (under discussion)
- Μη εφαρμόσιμο (not applicable)

3.2. Σχεδιασμός του Σχεδίου Ασφάλειας

Σχεδιάζεται το σχέδιο ασφάλειας που περιλαμβάνει:

- Το σχέδιο πολιτικής ασφάλειας
- Τους ρόλους και τις υποχρεώσεις του κάθε ρόλου
- Τα συμπληρωματικά έργα που απαιτούνται για την υλοποίηση της ασφάλειας.

Το προϊόν του τρίτου σταδίου είναι το Σχέδιο Ασφάλειας.

Πλεονεκτήματα της μεθόδου CRAMM:

1) Καλύπτει όλες τις φάσεις της ανάλυσης και διαχείρισης επικινδυνότητας
2) Καλύπτει όλες τις συνιστώσες ασφάλειας
3) Έχει δοκιμαστεί με επιτυχία και υπάρχει μεγάλη διεθνής εμπειρία
4) Συνοδεύεται από ειδικό εργαλείο λογισμικού που διευκολύνει την εφαρμογή της
5) Παρέχει μία μεγάλη βιβλιοθήκη αντιμέτρων.

Μειονεκτήματα της μεθόδου CRAMM:

1) Στηρίζεται σε μεγάλο βαθμό στη συνεργασία με τους χρήστες και τη διοίκηση του οργανισμού και τις δικές τους υποκειμενικές απόψεις
2) Έχει υψηλό κόστος εφαρμογής
3) Στηρίζεται σε ένα πολύ απλοϊκό μοντέλο του πληροφοριακού συστήματος
4) Εστιάζει μόνο στα δεδομένα και λαμβάνει υπόψη τους ανθρώπους μόνο ως πηγές απειλών
5) Απαιτεί αρκετές φορές την επέμβαση του αναλυτή και την προσαρμογή των αποτελεσμάτων των αυτόματων υπολογισμών
6) Το τελικό αποτέλεσμα στηρίζεται σε μεγάλο βαθμό σε υποκειμενικές εκτιμήσεις, οι οποίες όμως συχνά δεν γίνονται αντιληπτές ως υποκειμενικές
7) Απαιτεί επεξεργασία των προτεινόμενων αντιμέτρων για την προσαρμογή τους στα ιδιαίτερα χαρακτηριστικά του υπό μελέτη πληροφοριακού συστήματος. Τα περισσότερα αντίμετρα είναι πολύ γενικά.

4.2 Μέθοδος SBA

Η μέθοδος SBA (Security By Analysis) αναπτύχθηκε στις αρχές του 1980 στη Σουηδία και χρησιμοποιείται έκτοτε σχεδόν αποκλειστικά στις Σκανδιναβικές χώρες. Το βασικό χαρακτηριστικό της μεθόδου αυτής είναι ότι δέχεται πως οι άνθρωποι που συμμετέχουν στην καθημερινή λειτουργία ενός πληροφοριακού συστήματος έχουν τις περισσότερες πιθανότητες να εντοπίσουν προβλήματα που μπορεί να έχει και να προτείνουν λύσεις για αυτά.
Υπάρχουν διάφορες μέθοδοι SBA με κυριότερες τις SBA Check και SBA Scenario.

Η μέθοδος SBA Check κάνει ταχεία αποτίμηση του επιπέδου ασφάλειας ενός πληροφοριακού συστήματος, στηρίζεται σε ερωτηματολόγια και υποστηρίζεται από ειδικό λογισμικό.

Η μέθοδος SBA Scenario έχει τρεις επιλογές:

- Main analysis: γίνεται πλήρης ανάλυση του πληροφοριακού συστήματος με σκοπό τον προσδιορισμό της πιθανότητας πραγματοποίησης ενός κινδύνου ασφάλειας και την εκτίμηση του κόστους μέσω αναλυτικών αριθμητικών μεθόδων.
- Ten analysis: γίνεται ταχεία ανάλυση με την πιθανότητα και το κόστος να προσδιορίζονται στην κλίμακα 1:10.
- Risk window: γίνεται συνοπτική ανάλυση βασισμένη σε μία ποιοτική κλίμακα τεσσάρων βαθμίδων.

Η SBA Scenario αποτελείται από τέσσερα στάδια:

- Προετοιμασία (preparation): στο στάδιο αυτό συγκρούονται οι ομάδες ανάλυσης και διδασκαλίας της SBA. Ο ρόλος του ειδικού περιορίζεται στη διδασκαλία της μεθόδου και στον συντονισμό των εργασιών της ομάδας. Επίσης δημιουργείται το χρονοδιάγραμμα, γίνεται η καταγραφή, η οριοθέτηση και ο προσδιορισμός των ρόλων της ομάδας.
- Σενάρια (scenarios): στο στάδιο αυτό γίνεται ο εντοπισμός των πιθανών σεναρίων, η ανάλυση της επικινδυνότητας με αναλυτική περιγραφή του κάθε σεναρίου, η καταγραφή όλων των διαθέσιμων στοιχείων που αφορούν το σενάριο και η εκτίμηση της πιθανότητας πραγματοποίησης του κάθε σεναρίου. Επιπλέον, γίνεται η διαχείριση της επικινδυνότητας με προσδιορισμό των ευπαθειών που συνδέονται με το σενάριο, η επιλογή των αντιμέτρων και η κοστολόγηση τους.

- Σύνοψη (overview): στο στάδιο αυτό καθορίζονται οι προτεραιότητες υλοποίησης, οι προτεραιότητες βάσει των επιπτώσεων και οι προτεραιότητες βάσει της μείωσης της επικινδυνότητας που επιτυγχάνεται με την υλοποίηση του αντιμέτρου.
- Σχέδιο δράσης (action plan): στο στάδιο αυτό καταρτίζεται ένα συνολικό σχέδιο δράσης για την ασφάλεια του πληροφοριακού συστήματος και καθορίζονται οι υπεύθυνοι για την υλοποίηση των μέτρων προστασίας.

Πλεονεκτήματα της SBA μεθόδου:

1) Υιοθετεί μία ολιστική προσέγγιση (holistic approach) του ζητήματος της ασφάλειας
2) Η ανάλυση γίνεται από τους ίδιους ανθρώπους που χρησιμοποιούν καθημερινά το σύστημα
3) Είναι αρκετά απλή, κατανοητή από μη – ειδικούς και μπορεί να υλοποιηθεί με μικρό κόστος
4) Υποστηρίζεται από απλό και εύχρηστο λογισμικό.

Μειονεκτήματα της SBA μεθόδου:

1) Στηρίζεται σε μεγάλο βαθμό στις ικανότητες, τη φαντασία και στη διάθεση για συνεισφορά των ανθρώπων που εμπλέκονται
2) Προϋποθέτει την ανάπτυξη ανθρωποκεντρικής και συμμετοχικής κουλτούρας
3) Δεν παρέχει βιβλιοθήκες μέτρων προστασίας.

4.3 Μέθοδος MARION

Η MARION (Methodologie d' Analyse des Risques Informatiques et d' Optimisation par Niveau) είναι μία μέθοδος για την εκτίμηση των κινδύνων των πληροφοριακών συστημάτων. Αναπτύχθηκε από τον CLUSIF (Club de la Securite Informatique Francais) και εγκαταλείφθηκε το 1998 για μία άλλη μεθοδολογία, την MEHARI. Δίνει την ποσοτική αξιολόγηση των λογικών κινδύνων μιας εταιρίας στα διαφορετικά επίπεδα ασφάλειας. Η MARION βασίζεται στην αξιολόγηση των οργανωτικών και τεχνικών πτυχών της ασφάλειας.
Η μεθοδολογία βασίζεται σε ερωτηματολόγια ελέγχου που ασχολούνται με συγκεκριμένους τομείς. Τα ερωτηματολόγια βοηθούν να αξιολογηθούν τα τρωτά σημεία της εταιρίας στους συγκεκριμένους τομείς της ασφάλειας.
Βασίζονται σε εκατοντάδες ερωτήσεις με διαφορετικά βάρη. Η μεθοδολογία χρησιμοποιεί 27 δείκτες που κατατάσσονται σε 6 διαφορετικά θέματα. Κάθε ένα από αυτά παίρνει ένα βαθμό από 0 (καθόλου εξασφαλισμένο) έως 4 (άριστα εξασφαλισμένο).

Τα θέματα είναι:

- Οργάνωση της ασφάλειας
- Φυσική ασφάλεια
- Επιχειρησιακή ασφάλεια
- Λογική οργάνωση
- Λογική ασφάλεια
- Λογισμικό ασφαλείας

Η MARION έχει τέσσερα στάδια.

Φάση 0: προετοιμασία (preparation)

Σ' αυτό το στάδιο καθορίζονται οι διάφοροι στόχοι ασφάλειας που πρέπει να επιτευχθούν καθώς και το όριο της μελέτης. Αυτό το βήμα θα συμβάλει στην καλύτερη εφαρμογή της μεθόδου με τα καθορισμένα όρια.

Φάση 1: έλεγχος ευπάθειας (vulnerability audit)

Στο στάδιο αυτό απαντιούνται τα ερωτηματολόγια. Οι απαντήσεις θα βοηθήσουν στον εντοπισμό των διαφόρων κινδύνων σχετικά με την ασφάλεια του πληροφοριακού συστήματος. Στο τέλος του ελέγχου, φτιάχνεται ένα διάγραμμα που αντιπροσωπεύει τους βαθμούς που δίνονται για κάθε δείκτη υπογραμμίζοντας τους πιο σημαντικούς κινδύνους.

Φάση 2: αξιολόγηση κινδύνου (risk assessment)

Εδώ δίνεται προτεραιότητα στους κινδύνους σύμφωνα με την σημασία τους. Έπειτα, το πληροφοριακό σύστημα χωρίζεται σε διαφορετικούς φορείς για την λεπτομερέστερη ανάλυση του. Οι φορείς αυτοί ταξινομούνται σύμφωνα με τις απειλές, τις επιπτώσεις και τις πιθανότητες τους. Σ' αυτή τη μέθοδο ορίζονται 17 είδη απειλών.

Φάση 3: σχέδιο δράσης (action plan)

Το σχέδιο δράσης προτείνει διάφορες λύσεις ώστε να βελτιωθούν οι βαθμοί στους διάφορους τομείς. Ορισμένες λύσεις είναι τα προληπτικά μέτρα που μειώνουν την πιθανότητα εμφάνισης της απειλής, τα περιοριστικά μέτρα που μειώνουν τις επιπτώσεις. Επιπλέον, τα μέτρα ανίχνευσης που βοηθούν στην έγκαιρη ανίχνευση

και αντιμετώπιση μιας απειλής και τα μέτρα ανάκαμψης που βοηθούν στην αποκατάσταση της λειτουργίας του συστήματος.

Πλεονεκτήματα της μεθόδου MARION

1) Είναι εύκολη στην εφαρμογή, βασίζεται σε ερωτηματολόγια
2) Ίση βαρύτητα σε οργανωτικά και τεχνικά ζητήματα
3) Πετυχημένες τεχνικές παρουσίασης των αποτελεσμάτων της ανάλυσης

Μειονέκτημα της μεθόδου MARION

Απουσιάζει μία βιβλιοθήκη μέτρων προστασίας και μία αυστηρή μέθοδος επιλογή της.

4.4 Μέθοδος MEHARI

Η MEHARI (Methode Harmonisee d' Analyse de Risques) είναι μία μέθοδος αξιολόγησης κινδύνου και αναπτύχθηκε από την CLUSIF το 1996. Απευθύνεται κυρίως σε στελεχιακό δυναμικό (διευθυντές λειτουργίας, CISO, CIO, ελεγκτές, διευθυντής διαχείρισης κινδύνων) για τη διαχείριση της ασφάλειας των πληροφοριών και των πόρων των πληροφοριακών συστημάτων, και τη μείωση των κινδύνων. Η MEHARI είναι συμβατή με το πρότυπο διαχείρισης κινδύνου ISO/ IEC 27005 και είναι κατάλληλη για τη διαδικασία ISMS που περιγράφεται στο πρότυπο ISO 27001. Περιγράφει μία περίπλοκη διαδικασία συμπεριλαμβάνοντας τα κυκλικά βήματα της διαχείρισης κινδύνων καθώς και τη δημιουργία μιας προσαρμοσμένης βάσης γνώσεων. Μετά τη δημιουργία βάσης γνώσεων ξεκινάει μία διαδικασία για την ανάλυση των κινδύνων κάθε σεναρίου. Αυτή η διαδικασία ακολουθεί τα παρακάτω βήματα:

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

Πλεονεκτήματα της μεθόδου MEHARI

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

Μειονεκτήματα της μεθόδου MEHARI

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

4.5 Μέθοδος EBIOS

Η μέθοδος EBIOS (Expression des Besoins et Identification des Objectifs de Securite) αξιολογεί και ενεργεί τους κινδύνους σε σχέση με την ασφάλεια των πληροφοριακών συστημάτων. Η μέθοδος αυτή δημιουργήθηκε από τη Direction Centrale se la Securite des Systemes d' Information (DCSSI), ένα τμήμα του γαλλικού υπουργείου άμυνας και έχει ως στόχο κυρίως τη γαλλική διοίκηση.
Το ANSSI και ο σύλλογος EBIOS έχει κυκλοφορήσει μία νέα έκδοση του EBIOS που λαμβάνει υπόψη την εμπειρία ανατροφοδότησης και τις κανονιστικές αλλαγές. Η νέα μέθοδος είναι ευκολότερη, σαφέστερη και περιέχει παραδείγματα και συμβουλές. Προσφέρει τη δυνατότητα να αναπτύξουν και να παρακολουθούν ένα σχέδιο δράσης για την ασφάλεια των πληροφοριακών συστημάτων. Επίσης, περιλαμβάνει μία μελέτη περίπτωσης για την κατανόηση της μεθόδου.
Η EBIOS συνάδει με τα διεθνή πρότυπα ISO/IEC 31000, ISO/IEC 27001, ISO/IEC 27005, ISO/IEC 13335, ISO/IEC 15408, ISO/IEC 17799.
Η μέθοδος EBIOS παραμένει το βασικό πακέτο εργαλείων για οποιαδήποτε συζήτηση σχετικά με την ασφάλεια πληροφοριών.
Η EBIOS έχει πέντε ενότητες:

1. Μελέτη του πλαισίου
2. Μελέτη των ανεπιθύμητων ενεργειών
3. Μελέτη των σεναρίων για απειλές
4. Μελέτη της επικινδυνότητας
5. Μελέτη των μέτρων ασφάλειας

Μελέτη του πλαισίου

Αυτή η ενότητα έχει ως στόχο τη συλλογή στοιχείων που είναι απαραίτητα για τη διαχείριση κινδύνων. Προσαρμόζεται στο πλαίσιο της μελέτης και στα αποτελέσματά της ώστε να χρησιμοποιηθούν από τους ενδιαφερόμενους. Επιτρέπει την επισημοποίηση του πλαισίου διαχείρισης κινδύνων που διεξάγεται η μελέτη, καθώς και τον εντοπισμό, την

οριοθέτηση και την περιγραφή του πεδίου εφαρμογής της. Μετά την ολοκλήρωση αυτής της ενότητας περιγράφεται το σύνολο των παραμέτρων που περιλαμβάνονται σε άλλες ενότητες.
Η ενότητα αυτή έχει τρία στάδια:

- Ορισμός του πεδίου διαχείρισης κινδύνου
- Προετοιμασία μετρήσεων
- Προσδιορισμός των αγαθών

Μελέτη των ανεπιθύμητων ενεργειών/ Μελέτη των σεναρίων για απειλές

Οι ενότητες αυτές έχουν ως στόχο τον προσδιορισμό των γενικών σεναρίων των ανεπιθύμητων ενεργειών και απειλών. Επιτρέπουν την ανάδειξη όλων των ανεπιθύμητων συμβάντων εντοπίζοντας και συνδυάζοντας κάθε ένα από τα συστατικά του. Εκτιμάται η τιμή που είναι επιθυμητή για την προστασία και δείχνει τις πηγές των απειλών και τις συνέπειές τους. Είναι δυνατόν να εκτιμηθεί η σοβαρότητα και η πιθανότητα κάθε ανεπιθύμητης ενέργειας/ απειλής. Βοηθούν στον εντοπισμό των μέτρων ασφάλειας που ήδη υπάρχουν και αφού εφαρμοστούν επαναϋπολογίζεται επίδραση των συμβάντων. Μετά την ολοκλήρωση κάθε ενότητας, τα επίφοβα συμβάντα και οι απειλές αντίστοιχα προσδιορίζονται, εξηγούνται και τοποθετούνται με βάση τη πιθανότητα και τη σοβαρότητά τους.

Μελέτη της επικινδυνότητας

Στόχος αυτής της ενότητας είναι να αποδείξει τους συστηματικούς κινδύνους και να επιλέξει τον τρόπο επεξεργασίας λαμβάνοντας υπόψη τις ιδιαιτερότητες του πλαισίου. Συσχετίζοντας τα ανεπιθύμητα γεγονότα με τα σενάρια των απειλών που ενδέχεται να προκύψουν, αυτή η ενότητα επιτρέπει τον προσδιορισμό μόνο πραγματικών σεναρίων στο πεδίο εφαρμογής της μελέτης. Επίσης, μπορεί να δοθεί προτεραιότητα και να επιλεγεί η κατάλληλη θεραπεία. Μετά, την ολοκλήρωση της ενότητας, αξιολογούνται οι κίνδυνοι και οι θεραπευτικές επιλογές.
Η ενότητα αυτή έχει δύο στάδια:

- Αξιολόγηση των κινδύνων
- Προσδιορισμός των στόχων ασφάλειας

Μελέτη των μέτρων ασφάλειας

Στόχος της ενότητας είναι να καθοριστεί η αντιμετώπιση των κινδύνων και η παρακολούθηση της εφαρμογής τους. Επιτρέπει να επιτευχθεί συναίνεση σχετικά με τα μέτρα ασφάλειας που έχουν σχεδιαστεί για την αντιμετώπιση του κινδύνου που έχει

αναγνωριστεί προηγουμένως, αποδεικνύοντας τον σχεδιασμό, την υλοποίηση και την επικύρωση της θεραπείας. Μετά την ολοκλήρωση αυτής της ενότητας, προσδιορίζονται τα μέτρα ασφάλειας. Μπορεί επίσης να υλοποιηθεί και η παρακολούθηση της εφαρμογής. Η ενότητα αυτή έχει δύο στάδια:

- Επισημοποίηση των μέτρων ασφάλειας που πρέπει να εφαρμοστούν
- Εφαρμογή των μέτρων ασφάλειας

Πλεονεκτήματα της μεθόδου EBIOS

1) Γενική μέθοδος που επιτρέπει την ρύθμιση με τα τοπικά πρότυπα, συνήθειες, πλαίσιο
2) Μπορεί να εφαρμοστεί με τους στόχους της αξιολόγησης των διαφόρων μεγεθών και πολυπλοκότητας

Μειονέκτημα της μεθόδου EBIOS

1) Πιο αναλυτική τεκμηρίωση και υποστήριξη διαθέσιμο μόνο στα γαλλικά

4.6 Μέθοδος OCTAVE-S

Η OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) ορίζει μία στρατηγική αξιολόγησης κινδύνων των πληροφοριακών συστημάτων. Η OCTAVE είναι αυτοκατευθυνόμενη, δηλαδή άτομα από την οργάνωση αναλαμβάνουν την ευθύνη για τον καθορισμό στρατηγικής για την ασφάλεια ενάντια στους κινδύνους. Η OCTAVE-S είναι μία παραλλαγή προσαρμοσμένη στα περιορισμένα μέσα και τους περιορισμούς των μικρών οργανώσεων (έως 100 άτομα). Η OCTAVE-S οδηγείται από μία μικρή διεπιστημονική ομάδα, τρία με πέντε άτομα, από το προσωπικό του οργανισμού που συγκεντρώνει και αναλύει τα στοιχεία και παράγει στρατηγική για την προστασία και σχέδια μετριασμού βασισμένα στους λειτουργικούς κινδύνους του οργανισμού. Για την αποτελεσματική διεξαγωγή της OCTAVE-S η ομάδα πρέπει να έχει ευρεία γνώση των επιχειρηματικών δραστηριοτήτων και των διαδικασιών ασφάλειας του οργανισμού, έτσι ώστε να είναι σε θέση να διεξάγει όλες τις δραστηριότητες μόνη της. Οι μικρές οργανώσεις συχνά δεν έχουν αναπτύξει οργανωτικές ικανότητες για την εκτέλεση και την ερμηνεία των αποτελεσμάτων από τα εργαλεία αξιολόγησης της ευπάθειας. Έτσι, αντί να χρησιμοποιούν τα δεδομένα ευπάθειας για να βελτιώσουν την προβολή των τεχνικών της τρέχουσας ασφάλειας, εξετάζουν τις διαδικασίες που χρησιμοποιούνται για τη ρύθμιση και τη διατήρηση της υπολογιστικής υποδομής τους.

Εάν υπάρχουν ελλείψεις στην οργανωτική ικανότητα σημειώνονται και εξετάζονται κατά τη φάση 3 του OCTAVE-S όταν οργανισμός αναπτύσσει στρατηγική για την προστασία του.
Η OCTAVE-S έχει τρεις φάσεις:

Φάση 1: Δημιουργία αγαθού βασισμένο στα προφίλ των απειλών

Στη φάση 1 αξιολογούνται οι οργανωτικές πτυχές. Κατά τη διάρκεια αυτής της φάσης, η ομάδα ανάλυσης καθορίζει τα κριτήρια αξιολόγησης των επιπτώσεων που θα χρησιμοποιηθούν αργότερα για την αξιολόγηση των κινδύνων. Προσδιορίζει τα αγαθά και αξιολογεί την ασφάλεια της τρέχουσας πρακτικής του οργανισμού. Η ομάδα ολοκληρώνει όλες τις εργασίες συλλέγοντας πρόσθετες πληροφορίες μόνο όταν τις χρειάζεται. Στη συνέχεια επιλέγει τρία με πέντε κρίσιμα περιουσιακά στοιχεία και τα αναλύει σε βάθος με βάση την σημασία τους στον οργανισμό. Τέλος, η ομάδα ορίζει τις απαιτήσεις ασφάλειας και ένα προφίλ απειλών για κάθε κρίσιμο αγαθό.
Αυτή η φάση έχει δύο διαδικασίες.

1. Εντοπισμός των οργανωτικών πληροφοριών
    - Καθιέρωση κριτηρίων αξιολόγησης των επιπτώσεων
    - Προσδιορισμός οργανωτικών αγαθών
    - Αξιολόγηση οργανωτικών πρακτικών ασφάλειας
2. Δημιουργία προφίλ απειλών
    - Επιλογή κρίσιμου αγαθού
    - Προσδιορισμός απαιτήσεων ασφάλειας για τα κρίσιμα αγαθά
    - Προσδιορισμός απειλών για τα κρίσιμα αγαθά

Φάση 2: Προσδιορισμός ευπάθειας υποδομών

Κατά τη διάρκεια αυτής της φάσης, η ομάδα ανάλυσης διεξάγει μία ανασκόπηση υψηλού επιπέδου της υπολογιστικής υποδομής του οργανισμού. Αναλύει πως οι άνθρωποι χρησιμοποιούν την υπολογιστική υποδομή για να έχουν πρόσβαση σε αγαθά ζωτικής σημασίας, δίνοντας τις βασικές κατηγορίες των συστατικών καθώς και ποιος είναι υπεύθυνος για τη διαμόρφωση και τη διατήρηση των εν λόγω στοιχείων.

Η φάση 2 έχει μία διαδικασία.

1. Εξέταση υπολογιστικής υποδομής σε σχέση με κρίσιμα αγαθά

- Εξέταση προσπέλασης
- Ανάλυση τεχνολογίας με τις σχετικές διαδικασίες

Φάση 3: Ανάπτυξη σχεδίων και στρατηγικής για την ασφάλεια

Κατά τη διάρκεια της φάσης 3, η ομάδα ανάλυσης εντοπίζει τους κινδύνους για τα περιουσιακά στοιχεία του οργανισμού και αποφασίζει τι πρέπει να κάνει. Με βάση την ανάλυση των πληροφοριών που συγκεντρώθηκαν, η ομάδα δημιουργεί μία στρατηγική προστασίας για την οργάνωση και τα σχέδια μετριασμού των επιπτώσεων για την αντιμετώπιση των κινδύνων στα αγαθά. Τα φύλλα εργασία OCTAVE-S που χρησιμοποιούνται σε αυτή τη φάση είναι εξαιρετικά δομημένα και συνδεδεμένα με τον κατάλογο πρακτικών του OCTAVE, επιτρέποντας στην ομάδα να συσχετίσει τις συστάσεις για τη βελτίωση των πρακτικών ασφάλειας σε ένα αποδεκτό σημείο.
Αυτή η φάση έχει 2 διαδικασίες.

1. Προσδιορισμός και ανάλυση κινδύνων
    - Αξιολόγηση των επιπτώσεων των απειλών
    - Καθιέρωση κριτηρίων αξιολόγησης πιθανοτήτων
    - Αξιολόγηση των πιθανοτήτων των απειλών
2. Ανάπτυξη στρατηγικής προστασίας και σχεδίων μετριασμού επιπτώσεων
    - Περιγραφή στρατηγικής της τρέχουσας προστασίας
    - Επιλογή μετριασμού προσεγγίσεων
    - Ανάπτυξη σχεδίων μετριασμού των κινδύνων
    - Προσδιορισμός αλλαγών στην στρατηγική προστασίας
    - Προσδιορισμός επόμενων βημάτων

Πλεονεκτήματα της μεθόδου OCTAVE-S

1) Πραγματοποίηση από μικρές ομάδες των ιδίων εργαζομένων του οργανισμού
2) Περιέχει διάφορες μεθόδους προσαρμοσμένες για συγκεκριμένες οργανώσεις και πλαίσια
3) Ευρέως χρησιμοποιούμενη μέθοδος με αφθονία δικαιολογητικών και συμβατών εργαλείων τρίτων κατασκευαστών

Μειονέκτημα της μεθόδου OCTAVE-S

1) Είναι μία βαρέων βαρών μέθοδος που αποτελείται από πολλούς τόμους, φύλλα εργασίας και διαδικασίες.

Κεφάλαιο 5 ΠΡΑΚΤΙΚΟ ΜΕΡΟΣ

5.1 ΕΙΣΑΓΩΓΗ

Η μελέτη περίπτωσης που παρουσιάζεται σε αυτήν την ενότητα αφορά το τμήμα Πληροφορική με εφαρμογές στη Βιοϊατρική του πανεπιστημίου Θεσσαλίας. Σκοπός της είναι η εφαρμογή της ανάλυσης της επικινδυνότητας χρησιμοποιώντας το E-BIOS για την εξαγωγή συμπερασμάτων σε σχέση με το σύνολο των υπολογιστικών υποδομών του τμήματος.

Η μέθοδος EBIOS ,όπως αναφέρθηκε και παραπάνω, αξιολογεί και ενεργεί τους κινδύνους σε σχέση με την ασφάλεια των πληροφοριακών συστημάτων.

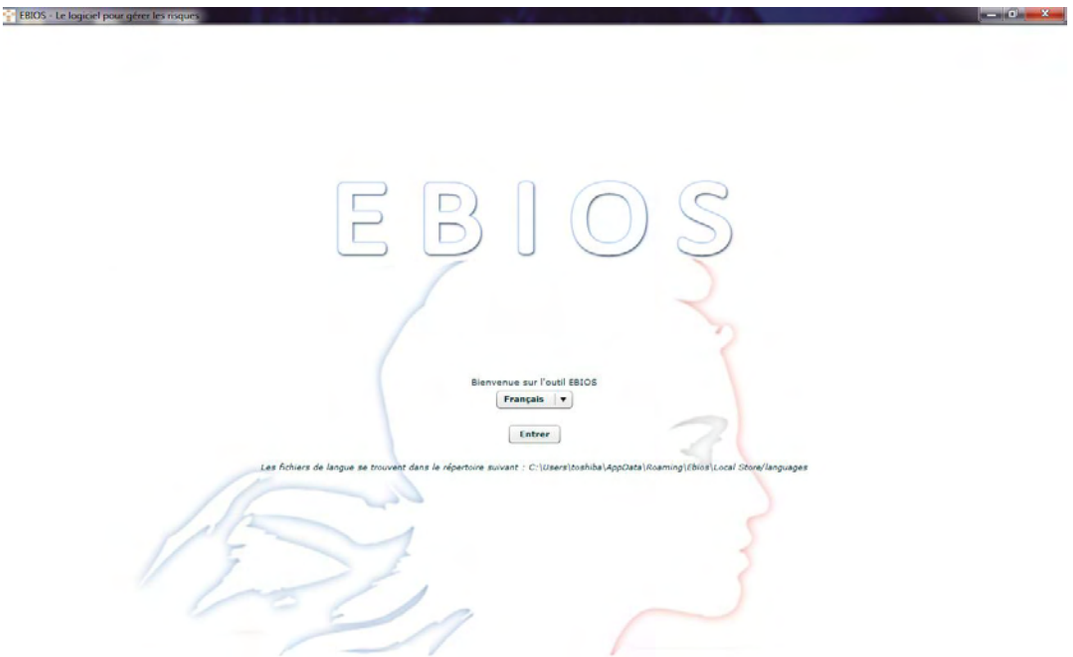
Η EBIOS έχει πέντε ενότητες:

1. Μελέτη του πλαισίου
2. Μελέτη των ανεπιθύμητων ενεργειών
3. Μελέτη των σεναρίων για απειλές
4. Μελέτη της επικινδυνότητας
5. Μελέτη των μέτρων ασφάλειας

5.2 ΕΦΑΡΜΟΓΗ ΑΝΑΛΥΣΗΣ ΚΑΙ ΔΙΑΧΕΙΡΙΣΗΣ ΚΙΝΔΥΝΟΥ ΣΤΟ ΤΜΗΜΑ ΤΟΥ ΠΑΝΕΠΙΣΤΗΜΙΟΥ ΜΕΣΩ ΤΗΣ ΜΕΘΟΔΟΥ EBIOS

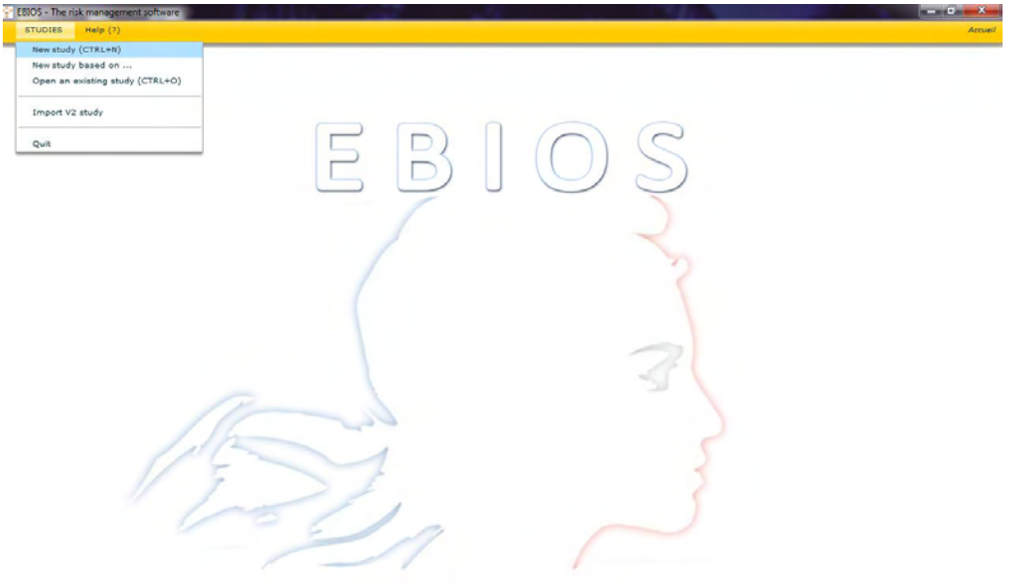
Το αρχείο είναι της μορφής ebios.air και η εγκατάστασή του είναι πολύ απλή.

1.Εναρξή του E-BIOS

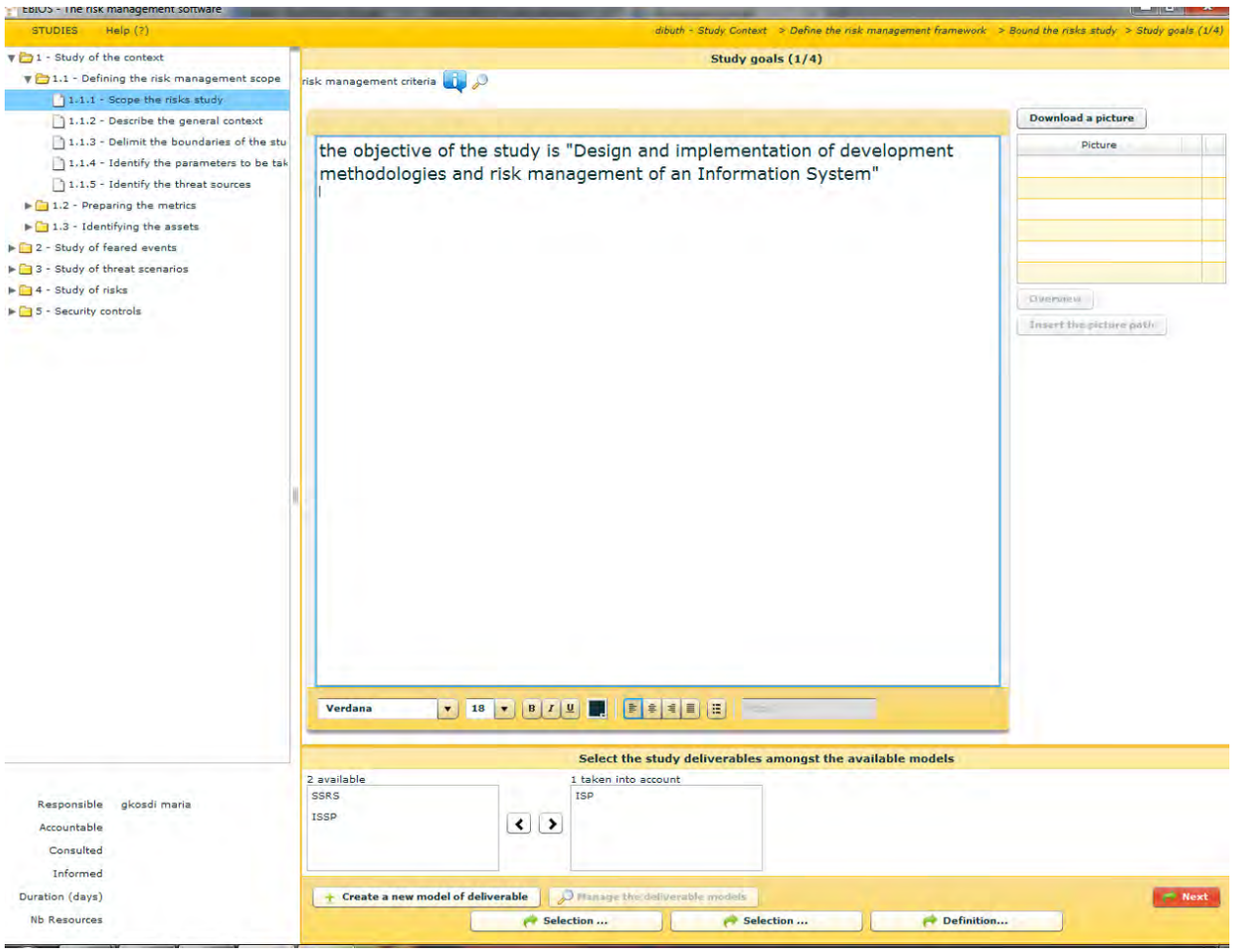


Επιλέγουμε τη γλώσσα: Αγγλικά ή Γαλλικά.

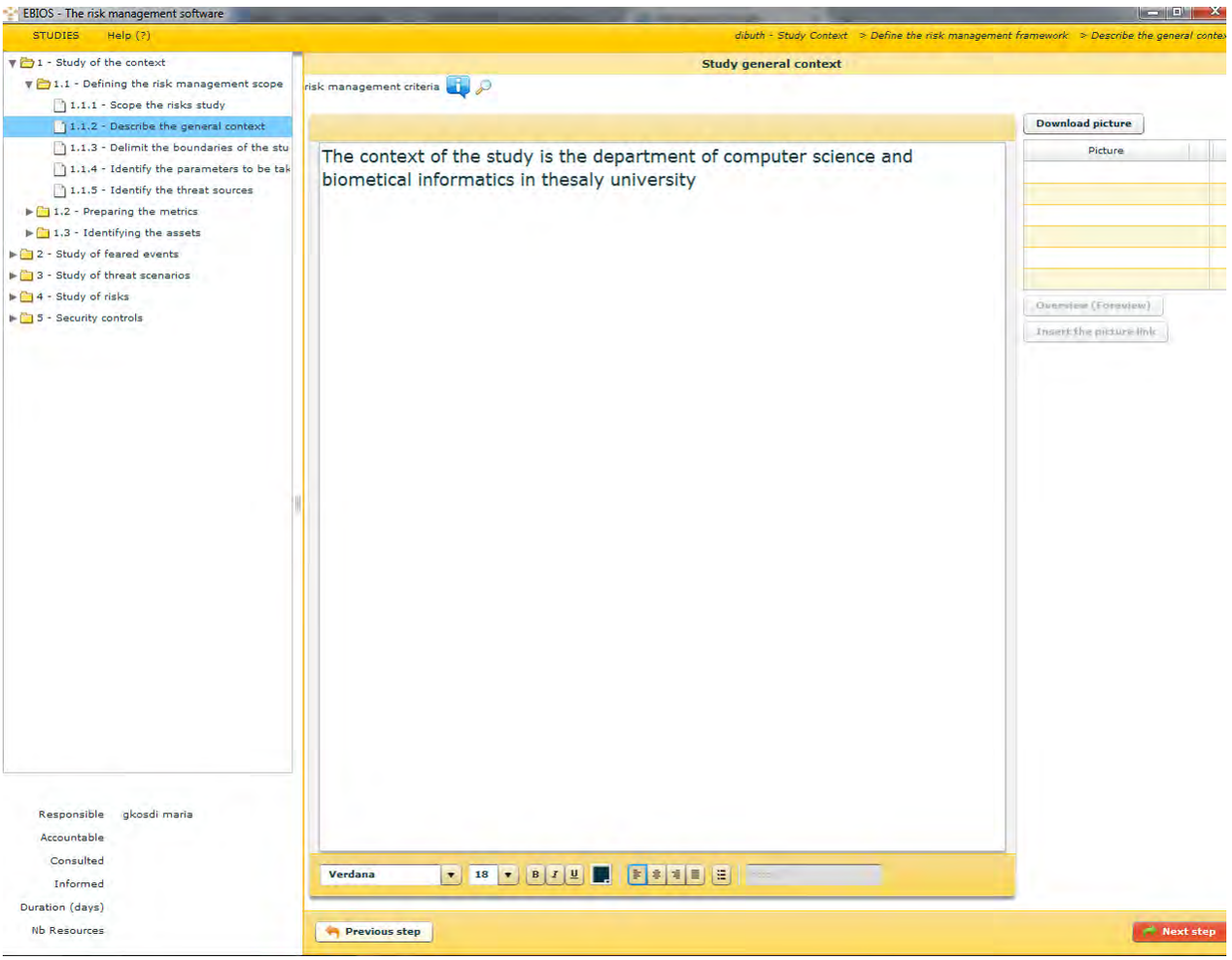
2.Επιλέγουμε new study και δημιουργούμε μία νέα μελέτη. Ορίζουμε τον τίτλο της μελέτης και επιλέγουμε που θα αποθηκευτεί.



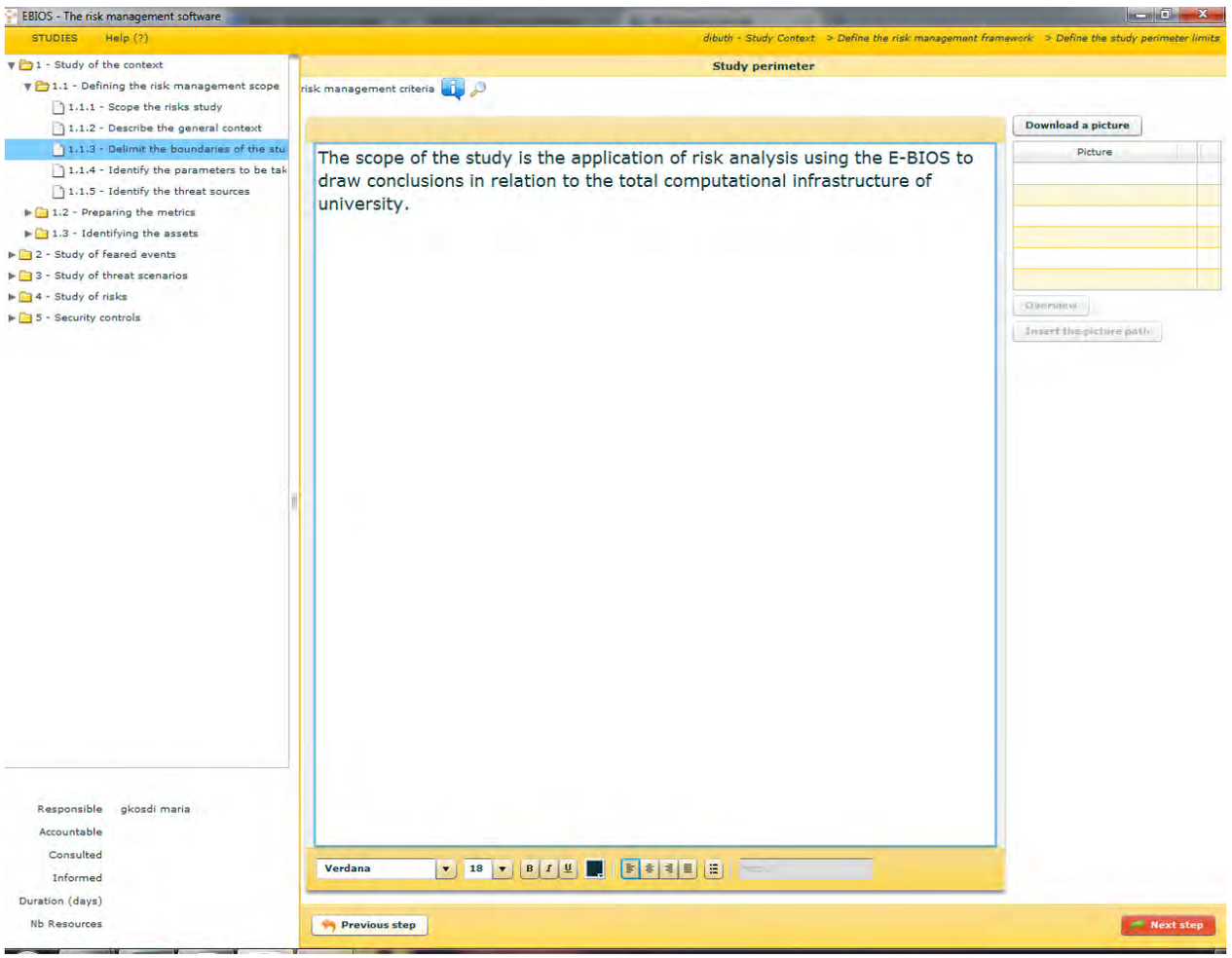
3.Στην ενότητα1.1.1.”πεδίο εφαρμογή της μελέτης κινδύνων “ γράφουμε τον στόχο της μελέτης



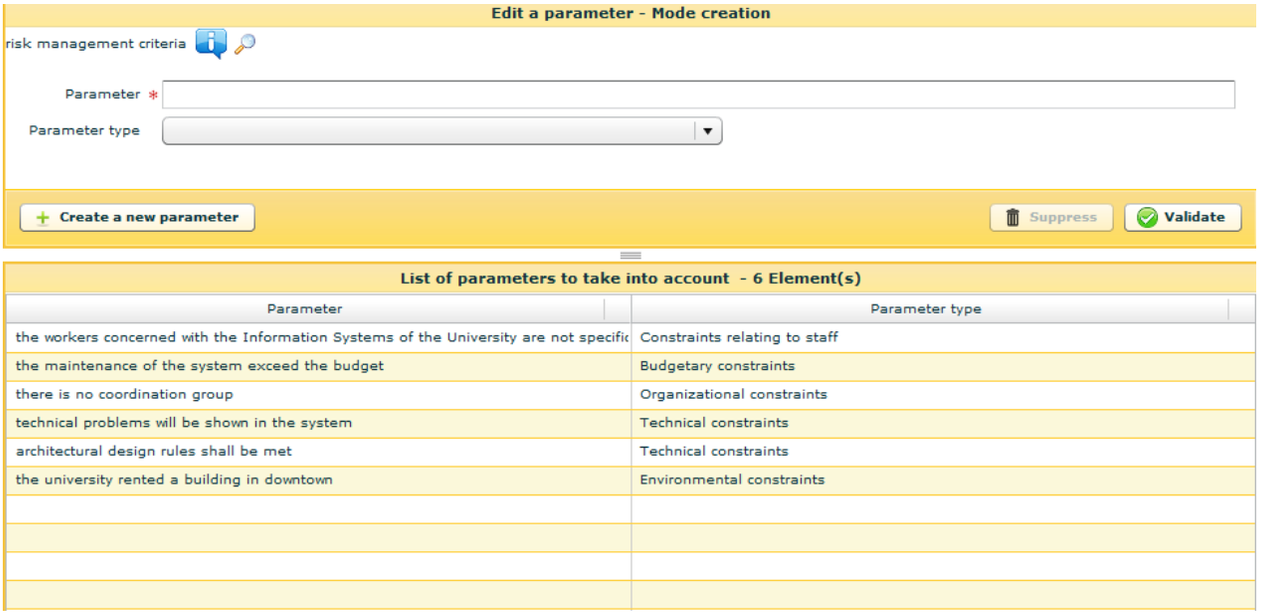
4.Η ενότητα 1.1.2. "περιγραφή του γενικού πλαισίου"



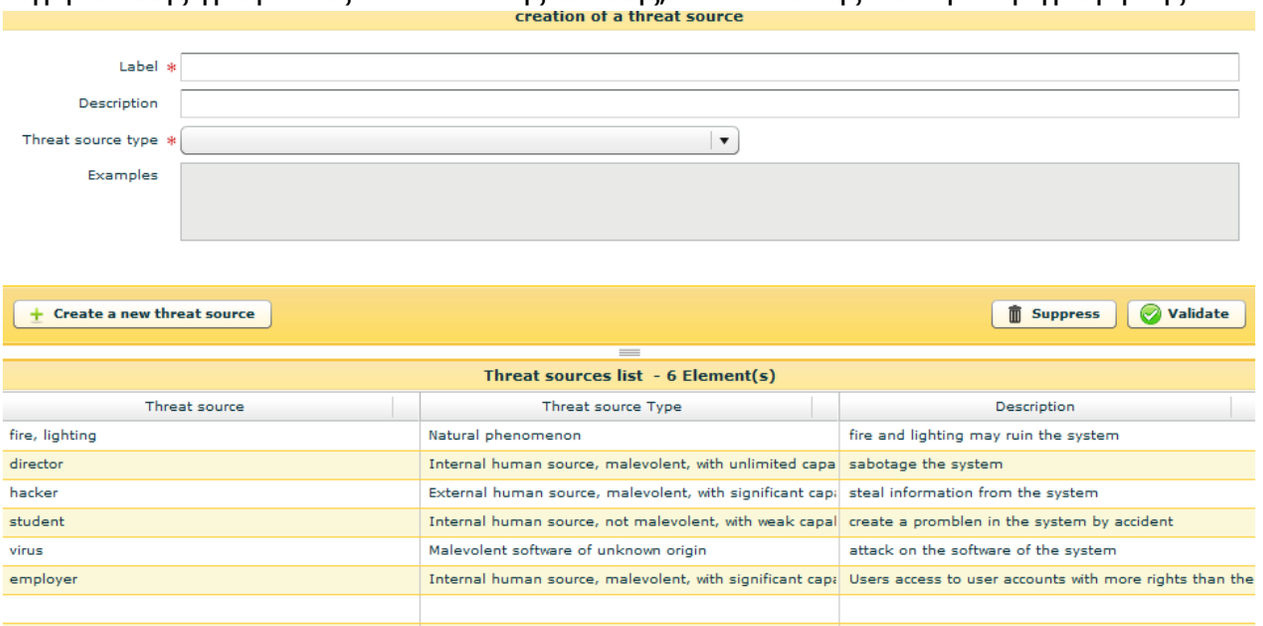
5.Η ενότητα 1.1.3. "οριοθέτηση της μελέτης"



6.Ενοτητα 1.1.4. "προσδιορισμός των παραμέτρων που πρέπει να ληφθούν" γράφουμε την παράμετρο και επιλέγουμε τον τύπο της.



7.Ενότητα1.1.5. "προσδιορισμός των πηγών των απειλών". Αρχικά δημιουργούμε μία νέα πηγή απειλής γράφοντας τον τίτλο της απειλής, τον τύπο της και την περιγραφή της.



Έπειτα επιλέγουμε τις πηγές που μας ενδιαφέρουν και αυτές μπαίνουν σε μία λίστα.

List of types for threat sources			
Threat source type	Selected	Threat Sources	rationale
Internal human source, malevolent, with			
Internal human source, malevolent, with	✓	employer	
Internal human source, malevolent, with	✓	director	
External human source, malevolent, with			
External human source, malevolent, with	✓	hacker	
External human source, malevolent, with			
Internal human source, not malevolent, w	✓	student	
Internal human source, not malevolent, w			
Internal human source, not malevolent, w			
External human source, not malevolent, w			
External human source, not malevolent, w			
External human source, not malevolent, w			
Malevolent software of unknown origin	✓	virus	
Natural phenomenon	✓	fire, lighting	
Natural or health disaster			
Animal activity			
Internal event			

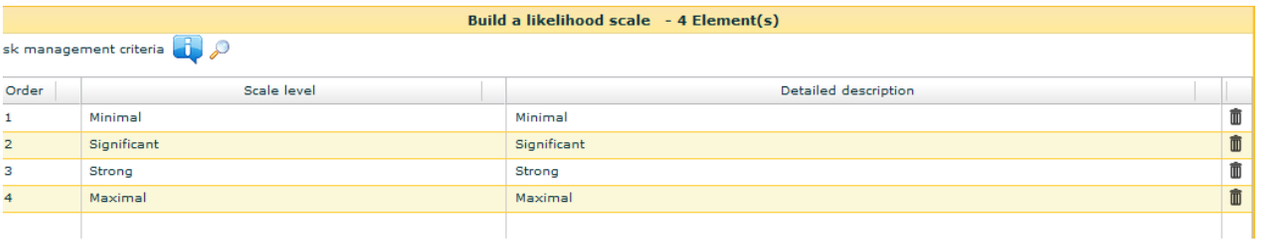
8.Λίστα των κριτηρίων ασφάλειας

List of security criteria - 3 Element(s)		
Security Criteria	Scale level	
Availability	1. More than 72h 2. Between 24h and 72h 3. Between 4h and 24h 4. Less than 4h	🗑
Confidentiality	1. Public 2. Limited 3. Reserved 4. Private	🗑
Integrity	1. Detectable 2. Controlled 3. Has Integrity	🗑

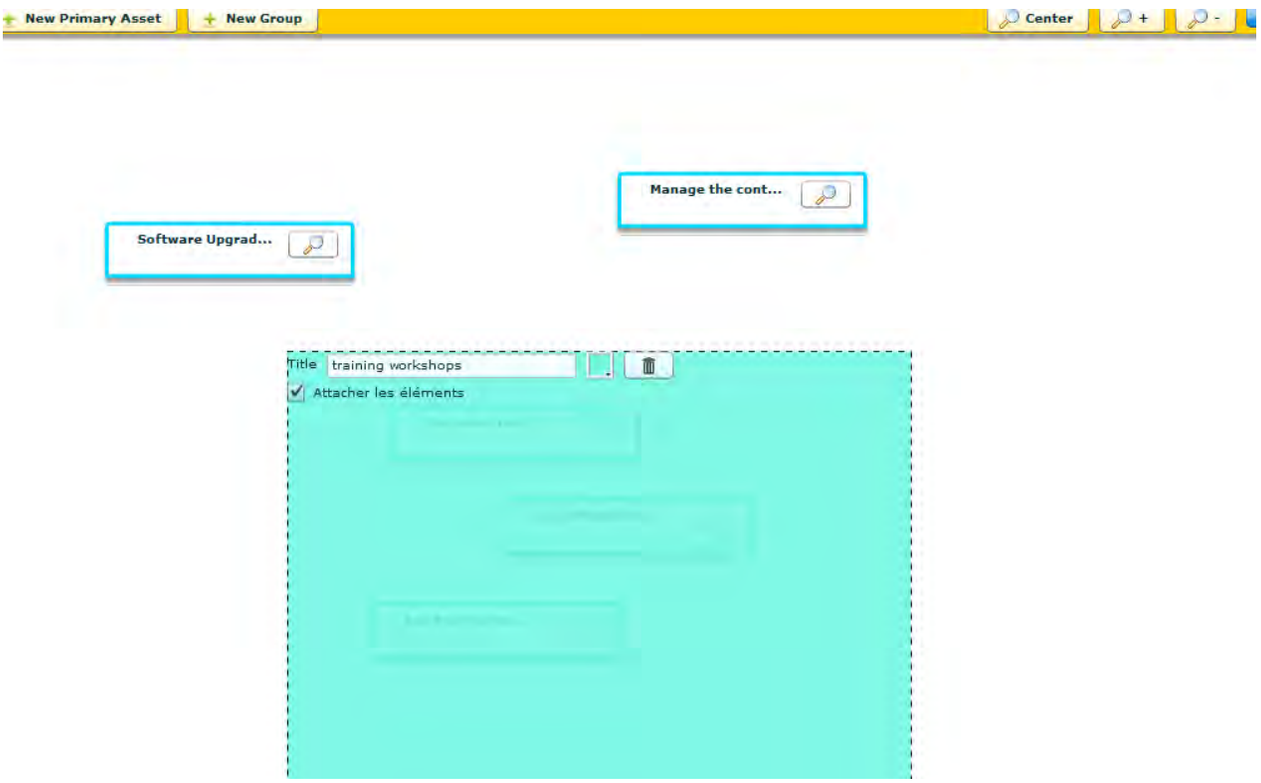
9.Λίστα της κλίμακας βαρύτητας

Build a gravity scale - 4 Element(s)			
risk management criteria			
Order	Scale level	Detailed description	
1	Negligible	Negligible severity	🗑
2	Limited	Limited severity	🗑
3	Important	Important severity	🗑
4	Critical	Critical severity	🗑

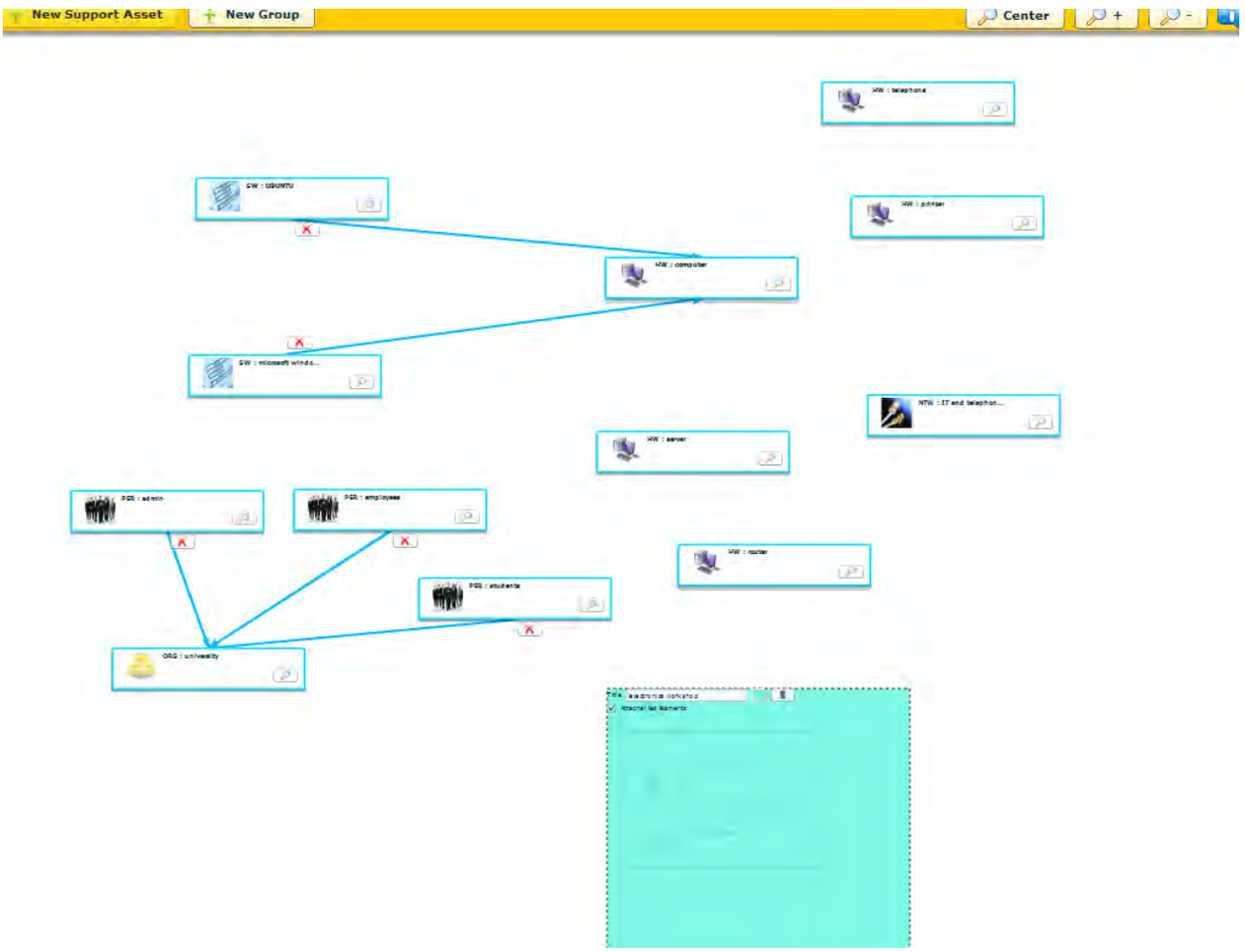
10.Λίστα της κλίμακας πιθανότητας



11.Προσδιορισμός των κύριων περιουσιακών στοιχείων



12.Προσδιορισμός των αγαθών υποστήριξης



13.Καθορισμός του συνδέσμου μεταξύ των κύριων αγαθών και των αγαθών υποστήριξης

risk management criteria

Select All

Support Asset	Manage the content...	educational worksho...	Electronic training...	two training worksh...	Software Upgrade
HW - server	☑	☑	☑	☑	☑
▼ HW - computer	☑	☑	☑	☑	☑
SW - microsoft wi	☑	☑	☑	☑	☑
SW - UBUNTU	☑	☑	☑	☑	☑
HW - printer	☑	☑	☑	☑	☑
HW - telephone	☑	☑	☑	☑	☐
HW - multimeter	☐	☐	☑	☐	☑
HW - generator	☐	☐	☑	☐	☑
HW - oscilloscope	☐	☐	☑	☐	☑
NTW - IT and telephi	☑	☑	☑	☑	☑
HW - router	☑	☑	☑	☑	☑
▼ ORG - university	☑	☑	☑	☑	☑
PER - admin	☑	☐	☐	☐	☑
PER - students	☐	☑	☑	☑	☐
PER - employees	☑	☑	☑	☑	☑

14. Λίστα με τα μέτρα ασφάλειας

List of Security measures - 4 Element(s)

Status (E/C)	Label	Measure Type	associated SA	Preventio	Protectior	Restorati
E	Agreement on the level of service by property	Controls of the study	university	X		X
E	Installing antivirus on Windows 7 and ubuntu	Controls of the study	microsoft windows 7 UBUNTU		X	
E	back up in the end of day	Controls of the study	admin employees			X
E	alarm when the university is closed	Controls of the study	university		X	

15.Αξιολόγηση των γεγονότων φόβου

Evaluation of feared events

risk management criteria 

Gravity	Feared Events
Critical	
Important	Electronic training workshop - Confidentiality Electronic training workshop - Integrity Manage the content of the website - Confidentiality Manage the content of the website - Integrity Software Upgrade - Availability Software Upgrade - Confidentiality Software Upgrade - Integrity educational workshop Image Processing - Availability educational workshop Image Processing - Confidentiality educational workshop Image Processing - Integrity two training workshops with computers - Availability two training workshops with computers - Confidentiality two training workshops with computers - Integrity
Limited	Electronic training workshop - Availability Manage the content of the website - Availability
Negligible	
Not retained	

16.Αξιολόγηση των σεναρίων απειλής

risk management criteria 

Likelihood level	Threat scenarios
Maximal	computer for programming - Availability
Strong	UBUNTU - Availability UBUNTU - Integrity admin - Availability computer for programming - Integrity microsoft windows 7 - Availability microsoft windows 7 - Integrity multimeter - Confidentiality server - Confidentiality
Significant	IT and telephony channels - Availability IT and telephony channels - Confidentiality IT and telephony channels - Integrity UBUNTU - Confidentiality admin - Confidentiality admin - Integrity computer for programming - Confidentiality employees - Availability employees - Confidentiality employees - Integrity generator - Availability generator - Confidentiality generator - Integrity microsoft windows 7 - Confidentiality multimeter - Availability multimeter - Integrity oscilloscope - Availability oscilloscope - Confidentiality oscilloscope - Integrity printer - Availability router - Availability router - Confidentiality router - Integrity server - Availability server - Integrity students - Availability students - Confidentiality students - Integrity telephone - Confidentiality university - Availability university - Integrity
Minimal	printer - Confidentiality printer - Integrity telephone - Availability telephone - Integrity university - Confidentiality
Not retained	

17.Αξιολόγηση των κινδύνων

18.Καθιιέρωση μιας δήλωσης της εφαρμογής

risk management criteria 

Type	Parameters	justification	Status
Constraints relating to staff	the workers concerned with the Information	The security measures by staff does not re	Satisfied
Budgetary constraints	the maintenance of the system exceed the	damages of equipement may exceed the b	Planned
Organizational constraints	there is no coordination group	there are promblems with responsibilities o	Satisfied
Technical constraints	technical problems will be shown in the syst	attack from hacker	Planned
Technical constraints	architectural design rules shall be met	unexpectable promblems in software	Planned
Environmental constraints	the university rented a building in downtowr	rent increases, eviction	Planned

19.Λίστα κινδύνων

Residual Risk	Feared Event	Threat scenario	Est. without measure		Est. with measures		Est. with complementary measures	
			Gravity	Likelihood	Gravity	Likelihood	Gravity	Likelihood
unavailability beyo	Manage the conte	server - Availabilit computer for prog printer - Availabilit telephone - Availa microsoft windows UBUNTU - Availabi IT and telephony router - Availabilit admin - Availabilit employees - Avail university - Availa	Limited	Maximal	Limited	Significant	Limited	Significant
non-intergrity cont	Manage the conte	server - Integrity computer for prog printer - Integrity telephone - Integ microsoft windows UBUNTU - Integrit IT and telephony router - Integrity admin - Integrity employees - Integ university - Integr	Important	Strong	Important	Significant	Important	Significant
confidentiality put	Manage the conte	server - Confident computer for prog printer - Confiden telephone - Confi microsoft windows UBUNTU - Confide IT and telephony router - Confident admin - Confident employees - Conf university - Confic	Important	Strong	Important	Significant	Important	Significant
unavailability beyo	educational works	server - Availabilit computer for prog printer - Availabilit telephone - Availa microsoft windows UBUNTU - Availabi IT and telephony router - Availabilit students - Availab employees - Avail university - Availa	Important	Maximal	Important	Significant	Important	Significant
non-intergrity cont	educational works	server - Integrity computer for prog printer - Integrity telephone - Integ microsoft windows UBUNTU - Integrit IT and telephony router - Integrity	Important	Strong	Important	Significant	Important	Significant

Εικόνα 1

Residual Risk	Feared Event	Threat scenario	Est. without measure		Est. with measures		Est. with complementary measures	
			Gravity	Likelihood	Gravity	Likelihood	Gravity	Likelihood
confidentiality put	educational works	server - Confident computer for prog printer - Confiden telephone - Confi microsoft windows UBUNTU - Confide IT and telephony router - Confident students - Confide employees - Conf university - Confic	Important	Strong	Important	Minimal	Important	Minimal
unavailability beyo	Electronic training	server - Availabilit computer for prog printer - Availabilit telephone - Availa multimeter - Avail generator - Availa oscilloscope - Ava microsoft windows UBUNTU - Availabi IT and telephony router - Availabilit students - Availab employees - Avail university - Availa	Limited	Maximal	Limited	Significant	Limited	Significant
non-intergrity cont	Electronic training	server - Integrity computer for prog printer - Integrity telephone - Integ multimeter - Integ generator - Integr oscilloscope - Inte microsoft windows UBUNTU - Integrit IT and telephony router - Integrity students - Integrit employees - Integ university - Integr	Important	Strong	Important	Significant	Important	Significant
confidentiality put	Electronic training	server - Confident computer for prog printer - Confiden telephone - Confi multimeter - Conf generator - Confic oscilloscope - Con microsoft windows UBUNTU - Confide IT and telephony router - Confident students - Confide employees - Conf university - Confic	Important	Strong	Important	Strong	Important	Strong

Εικόνα 2

Residual Risk	Feared Event	Threat scenario	Est. without measure		Est. with measures		Est. with complementary measures	
			Gravity	Likelihood	Gravity	Likelihood	Gravity	Likelihood
unavailability beyc	two training works	server - Availabilit computer for prog printer - Availabilit telephone - Availa microsoft windows UBUNTU - Availabi IT and telephony router - Availabilit students - Availab employees - Avail university - Availa	Important	Maximal	Important	Strong	Important	Strong
non-intergrity cont	two training works	server - Integrity computer for prog printer - Integrity telephone - Integ microsoft windows UBUNTU - Integrit IT and telephony router - Integrity students - Integrit employees - Integ university - Integr	Important	Strong	Important	Strong	Important	Strong
confidentiality put	two training works	server - Confident computer for prog printer - Confiden telephone - Confi microsoft windows UBUNTU - Confide IT and telephony router - Confident students - Confide employees - Conf university - Confic	Important	Strong	Important	Significant	Important	Significant

Εικόνα 3

unavailability beyc	Software Upgrade	server - Availabilit computer for prog printer - Availabilit multimeter - Avail generator - Availa oscilloscope - Ava microsoft windows UBUNTU - Availabi IT and telephony router - Availabilit admin - Availabilit employees - Avail university - Availa	Important	Maximal	Important	Strong	Important	Strong
non-intergrity conf	Software Upgrade	server - Integrity computer for prog printer - Integrity multimeter - Integ generator - Integr oscilloscope - Inte microsoft windows UBUNTU - Integrit IT and telephony router - Integrity admin - Integrity employees - Integ university - Integr	Important	Strong	Important	Strong	Important	Strong
confidentiality put	Software Upgrade	server - Confident computer for prog printer - Confiden multimeter - Conf generator - Confic oscilloscope - Con microsoft windows UBUNTU - Confide IT and telephony router - Confident admin - Confident employees - Conf university - Confic	Important	Strong	Important	Strong	Important	Strong

Εικόνα 4

Κεφάλαιο 6 ΣΥΜΠΕΡΑΣΜΑΤΑ

Η E-BIOS είναι το βασικό πακέτο εργαλείων για οποιαδήποτε συζήτηση σχετικά με την ασφάλεια πληροφοριών. Προσφέρει τη δυνατότητα ανάπτυξης και παρακολούθησης ενός σχεδίου δράσης για την ασφάλεια των πληροφοριακών συστημάτων.
Τα αποτελέσματα ανάλυσης και διαχείρισης των κινδύνων με τη βοήθεια του εργαλείου E-BIOS είναι η συλλογή, η εκτίμησης και η συνεχής παρακολούθηση των κινδύνων που εμφανίζονται. Σε μία λίστα προσδιορίζονται τα γεγονότα φόβου και τα σενάρια απειλών. Τέλος, προσδιορίζεται η βαρύτητα κάθε σεναρίου καθώς και η πιθανότητα εμφάνισης του, με και χωρίς την εγκατάσταση μέτρων ασφαλείας.
Για να προληφθούν τα προβλήματα από την παρουσίαση των κινδύνων θα πρέπει να υπάρχει προληπτική ανάλυση καθώς και συνεχή ενημέρωση της λίστας των κινδύνων. Ένα σχέδιο διαχείρισης και η λίστα των κινδύνων θα εκθέσει τα δυνατά και τα αδύναμα σημεία του τμήματος. Έτσι, οι διαχειριστές θα μπορούν να προσδιορίσουν ποιοι κίνδυνοι μπορούν να αποφευχθούν, ποιοι να μετριαστούν και ποιοι να γίνουν αποδεκτοί.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] Τσουμα Β.(2007). Διαχειριση Ασφαλειας Πληροφοριακων Συστηματων με Οντολογιες. Διατριβη, Τμημα Πληροφορικης, Οικονομικο Πανεπιστημιο Αθηνων.

[2] Λερα Μ.(2012). Μελετη Ασφαλειας Πληροφοριων και Πληροφοριακων Συστηματων. Διπλωματικη εργασια, Τμημα Μηχανικων Πληροφορικης και Τηλεπικοινωνιων, Πανεπιστημιο Δυτικης Μακεδονιας.

[3] Γεωργιου Σ.(2012). Αναλυση και Διαχειριση Επικινδυνοτητας στα Πληροφοριακα Συστηματα – Υλοποιηση Μεθοδολογιας σε Επιχειρησιακο Παραβαλλον. Μεταπτυχιακη εργασια, Τμημα Πληροφορικης, Πανεπιστημιο Πειραιως

[4] Γεωργιου Ν.(2004). Αναλυση Κινδυνων Πληροφοριακων Συστηματων. Διπλωματικη εργασια, Τμημα Ηλεκτρολογων Μηχανικων και Μηχανικων Υπολογιστων, Αριστοτελειο Πανεπιστημιο Θεσσαλονικης

[5] Αλεξακη Ε.(2008). Καταγραφη πολιτικων ασφαλειας συμφωνα με το προτυπο ISO 27002. Πτυχιακη εργασια, Τμημα Εφαρμοσμενης Πληροφορικης και Πολυμεσων, Τεχνολογικο Εκπαιδευτικο Ίδρυμα Κρητης

[6] IT risk management. www.en.wikipedia.org/wiki/IT_risk_management

[7] Risk Management: Certified ISO 27005 Risk Manager. IMF International Management Forum www.imfacademy.com/areasofexpertise/information_technology/certified_risk_management.php

[8] ISO/IEC 27001:2005 www.en.wikipedia.org/wiki/ISO/IEC_27001:2005

[9] ISO/IEC 27001:2013 www.en.wikipedia.org/wiki/ISO/IEC_27001:2013

[10] (2009). Εκπονηση Συνοπτικης Μελετης Αναλυσης και Διαχειρισης Επικινδυνοτητας. Εργαστηριακη ασκηση, Τμημα Διδακτικης της Τεχνολογιας και Ψηφιακων Συστηματων, Πανεπιστημιο Πειραιως

[11] Λαβδιωτη Μ.(2012). Μελετη παραγοντων Risk Management και αναπτυξη συστηματος. Διπλωματικη Εργασια, Τμημα Ψηφιακων Συστηματων, Πανεπιστημιο Πειραιως

[12] Lefebvre N.(2007). Creation of a Risk Assessment Methodology. Master of Science Thesis, Royal Institute of Technology, Stockholm

[13] Dan Ionita(2013). Current Established Risk Assessment Methodologies and Tools. Master Thesis, Universiteit Twente

[14] (2010). MEHARI 2010 Risk analysis and treatment Guide, CLUSIF

[15] EBIOS COMPLIANCE, ISDecisions www.isdecisions.com/compliance/EBIOS-compliance.htm

[16] EBIOS 2010 – Expression of Needs and Identification of Security Objectives, ANSSI www.ssi.gouv.fr/en/the-anssi/publications-109/methods-to-achive-iss/ebios-2010-expession-of-needs-and-identifications-of-security-objectives.html

[17] (2010). EBIOS Methode de Gestion des Risques. ANSSI

[18] Alberts C. & Dorofee A. & Stevens J. & Woody C.(2005). OCTAVE-S Implementation Guide, Version 1.0. Carnegie Mellon Software Engineering Institute

[19] Μαγκος Ε.(2007). Ασφαλεια Υπολογιστων και Προστασια Δεδομενων. Σημειωσεις μαθηματος, Τμημα Πληροφορικης, Ιονιο Πανεπιστημιο

[20] Fundamentals of Information Systems Security/Information Security and Risk Management

[21] http://en.wikibooks.org/wiki/Fundamentals_of_Information_Systems_Security/Information_Security_and_Risk_Management#Risk_Assessment.2FAnalysis

[22] Jerkins B.D. SECURITY RISK ANALYSIS AND MANAGEMENT, Countermeasures, INC. www.nr.no/~abie/RA_BY_jERKINS

[23] Μπολλας Γ.(2009). "Ηλεκτρονικη υγεια: Υφιστάμενη κατασταση και μελλοντικες εξελιξεις". Τμημα Ηλεκτρολογων Μηχανικων και Μηχανικων Υπολογιστων, Εθνικο Μετσοβιο Πανεπιστημιο

[24] Antonatos S.(2009). Defending against known and unknown attacks using a Network of Affined Honeypots. Doctoral Dissertation, Computer Science Department, University of Crete