ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΠΑΤΡΩΝ
ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ & ΟΙΚΟΝΟΜΙΑΣ
ΤΜΗΜΑ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΑΝΑΛΥΣΗ , ΑΠΟΤΙΜΗΣΗ & ΔΙΑΧΕΙΡΙΣΗ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ ΣΤΑ ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ (mis). ΠΑΡΟΥΣΙΑΣΗ ΜΙΑΣ ΜΕΘΟΔΟΛΟΓΙΑΣ ΔΙΑΧΕΙΡΙΣΗΣ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ.

ΣΠΟΥΔΑΣΤΡΙΑ : ΚΟΤΣΙΟΥΡΟΥ ΣΤΑΜΑΤΙΝΑ (Α.Μ.7233)
ΕΠΟΠΤΕΥΩΝ ΚΑΘΗΓΗΤΗΣ : ΑΓΓΕΛΟΠΟΥΛΟΣ ΙΩΑΝΝΗΣ

ΠΑΤΡΑ , ΦΕΒΡΟΥΑΡΙΟΣ 2011

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΡΟΛΟΓΟΣ

Στα πλαίσια της πτυχιακής εργασίας ασχολήθηκα με το θέμα της Ανάλυσης, Αποτίμησης και Διαχείρισης Επικινδυνότητας στα Πληροφοριακά Συστήματα (mis) που εντάσσεται στον ευρύτερο τομέα της ασφάλειας των ΠΣ. Στοχεύοντας στο να κατανοήσουμε καλύτερα την ουσία του θέματος, παρουσιάζεται μία από τις πλέον διαδεδομένες μεθοδολογίες για τον σχεδιασμό και την διαχείριση της ασφάλειας ενός ΠΣ, η μεθοδολογία ανάλυσης και διαχείρισης επικινδυνότητας.

Αναλυτικότερα, θα λέγαμε ότι στο 1^0 κεφάλαιο γίνεται μία εισαγωγή του θέματος στοχεύοντας στο να κατανοήσει ο αναγνώστης την ανάγκη για ασφάλεια που απαιτείται στα ΠΣ καθώς και τους τρεις στόχους της ασφάλειας

- ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑ
- ΑΚΕΡΑΙΟΤΗΤΑ
- ΔΙΑΘΕΣΙΜΟΤΗΤΑ

Επιπλέον, δίνεται μία συνοπτική εικόνα των Πολιτικών Ασφάλειας.

Στο 2^o κεφάλαιο, συγκεκριμενοποιείται η έννοια της ασφάλειας στο ΠΣ η οποία μας ωθεί στην περαιτέρω ανάλυση της έννοιας του κινδύνου. Παρουσιάζονται επίσης, τα είδη του κινδύνου, οι απώλειες που προκύπτουν από την πρόκληση του κινδύνου κ στο τέλος του κεφαλαίου αναλύεται η έννοια της επικινδυνότητας.

Στο επόμενο κεφάλαιο ,το 3^o, αναλύεται η μεθοδολογία Ανάλυσης και Διαχείρισης Επικινδυνότητας, παρουσιάζονται κάποια πλεονεκτήματα και μειονεκτήματα της μεθόδου, αναφέρονται και τέσσερις διαδεδομένες μεθοδολογίες που παρουσιάζονται αναλυτικά. Επιπλέον, στο ίδιο κεφάλαιο παρουσιάζονται και τα λογισμικά ανάλυσης κινδύνου.

Στο 4^{ο} κεφάλαιο γίνεται αναφορά στα Μοντέλα Διαχείρισης Επικινδυνότητας και παρουσιάζονται δυο από αυτά περιληπτικά. Ολοκληρώνοντας την εργασία στο 5^{ο} κεφάλαιο γίνεται η σύγκριση των μεθοδολογιών που αναλύσαμε και μία προσπάθεια παρουσίασης του τρόπου επιλογής της κατάλληλης μεθόδου και ακολούθως το 6^{ο} κεφάλαιο όπου είναι τα συμπεράσματα δηλαδή οι τελικές σκέψεις για αυτό που αποκομίσαμε από την εργασία.

ΚΕΦΑΛΑΙΟ 1

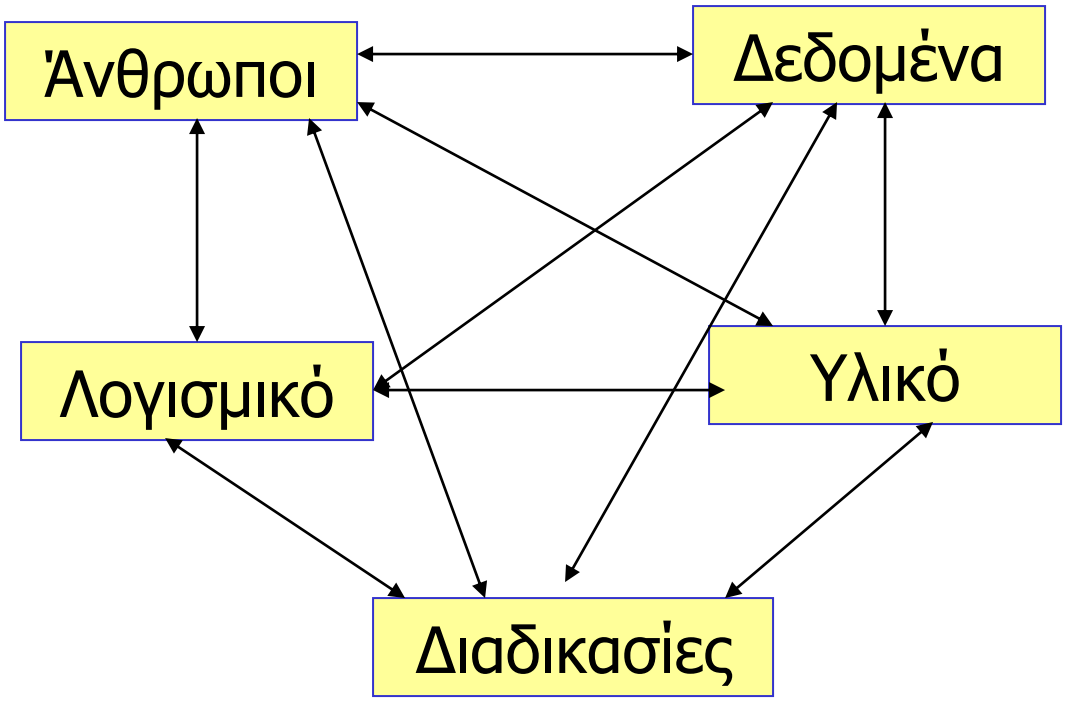
ΕΙΣΑΓΩΓΗ

Παραδοσιακά, οι συντελεστές παραγωγής περιελάμβαναν το κεφάλαιο, το ανθρώπινο δυναμικό, την γη. Πρόσφατα, στους συντελεστές παραγωγής έχει προστεθεί και η πληροφορία. Χωρίς έγκαιρη και έγκυρη πληροφορία πολλές επιχειρήσεις δεν θα μπορούσαν να λειτουργήσουν.

Τα σύγχρονα πληροφοριακά συστήματα που βασίζονται στον ηλεκτρονικό υπολογιστή (Η/Υ) συλλέγουν, αποθηκεύουν, αναλύουν και διαχέουν δεδομένα και πληροφορίες. Με τον τρόπο αυτό υποστηρίζουν τις λειτουργίες μίας επιχείρησης και παρέχουν τις πληροφορίες που χρειάζονται στην διοίκησή της για αποτελεσματικότερες αποφάσεις.

Πληροφοριακό σύστημα σημαίνει ότι ένας αριθμός αλληλεπιδρώντων στοιχείων έχουν οργανικά συναρμολογηθεί σε μια ολότητα, έτσι ώστε να εκτελέσουν μια ορισμένη λειτουργία. Τα στοιχεία αυτά είναι :

- Άνθρωποι
- Δεδομένα
- Λογισμικό
- Υλικός εξοπλισμός και
- Διαδικασίες



(Σχ.1 Συνιστώσες ενός πληροφοριακού συστήματος)

Εξαιτίας του ρόλου που παίζει το Π.Σ. σε μια επιχείρηση και όχι μόνο, είναι φυσικό να απαιτεί ασφάλεια και προστασία. Συνεπώς τα Π.Σ. θα πρέπει να προστατεύονται από κάθε μορφή απειλής, χωρίς όμως η προστασία αυτή να παρεμποδίζει τη ροή των πληροφοριών.

1.1 Η ανάγκη για ασφάλεια

Στην σύγχρονη εποχή, η χρήση των πληροφοριακών συστημάτων είναι δεδομένη για κάθε οργανισμό. Η επανάσταση της συνδεσιμότητας είναι πλέον γεγονός. Η ελεύθερη ροή πληροφοριών, οι ευκολίες που παρέχει το Internet καθώς και το ηλεκτρονικό εμπόριο έχουν ωθήσει μέχρι και τις μικρότερες επιχειρήσεις να επενδύσουν στην χρήση πληροφοριακών συστημάτων και διαδικτυακών εφαρμογών. Σαν αποτέλεσμα, στο μεγαλύτερο ποσοστό των οργανισμών η χρήση των πληροφοριακών συστημάτων είναι απολύτως αναγκαία για την επίτευξη των στόχων και της βασικής λειτουργικότητας τους. Έτσι, η παραμικρή δυσλειτουργία, διακοπή ή παράνομη διείσδυση στα συστήματα αυτά μεταφράζεται σε κόστος, είτε από άμεσες οικονομικές απώλειες, είτε από την αδυναμία του οργανισμού να λειτουργήσει αποδοτικά.

Εκτός από τις οικονομικές επιπτώσεις όμως, τα προβλήματα ασφαλείας πληροφοριακών συστημάτων γίνονται ακόμα πιο αισθητά σε συστήματα που περιέχουν ευαίσθητα δεδομένα ή επιτελούν «ευαίσθητες» και σημαντικές λειτουργίες. Διάφορα παραδείγματα τέτοιων συστημάτων είναι:

- Συστήματα με απόρρητα στρατιωτικά δεδομένα
- Συστήματα ελέγχου εναέριας κυκλοφορίας
- Συστήματα με ευαίσθητα ιατρικά δεδομένα
- Συστήματα που περιέχουν ευαίσθητα προσωπικά δεδομένα

Είναι φανερό ότι η ρήξη της ασφάλειας τέτοιων πληροφοριακών συστημάτων μπορεί να προκαλέσει σοβαρότατα προβλήματα που απειλούν άμεσα την ανθρώπινη ζωή και την ασφάλεια σε τοπικό, εθνικό αλλά και σε παγκόσμιο επίπεδο. Δεν υπάρχει λοιπόν αμφιβολία ότι η ασφάλεια των πληροφοριακών συστημάτων έχει τεράστια σημασία στην σύγχρονη κοινωνία και πρέπει να παίζει πρωτεύον ρόλο κατά την σχεδίαση, συντήρηση και χρήση τους.

Το πρόβλημα της ασφάλειας αφορά ανθρώπους και όχι συστήματα ή τεχνολογίες .Οι τεχνικές λύσεις αντιμετωπίζουν ένα μέρος του προβλήματος,

Επιπλέον, συνήθως οι χρήστες έχουν συγκεκριμένες απαιτήσεις για την ασφάλεια αλλά όχι εξειδικευμένες γνώσεις.

Εντούτοις, συμπεραίνουμε ότι η ασφάλεια είναι μια πορεία και όχι μια κατάσταση, συνεπώς δεν γίνεται να λύσουμε όλα τα προβλήματα της ασφάλειας και μετά να μείνουμε ήσυχοι.

Καθώς τα Π.Σ διαρκώς μεταβάλλονται, οι επιτιθέμενοι είναι ευρηματικοί και οι απειλές αλλάζουν ταχύτατα είναι επιβεβλημένο οι μέθοδοι προστασίας να ενημερώνονται συνεχώς και ακατάπαυστα.

1.2 Στόχος ασφάλειας ενός πληροφοριακού συστήματος

Στόχος της ασφάλειας ενός ***υπολογιστικού συστήματος***

- Διαφύλαξη των υπολογιστικών πόρων έναντι μη εξουσιοδοτημένης ή κακής χρήσης τους
- Προστασία πληροφορίας ή δεδομένων που κωδικοποιούν την πληροφορία από ακούσια ή σκόπιμη βλάβη, αποκάλυψη ή τροποποίησή τους

Μια αναγκαία συνθήκη για να είναι δυνατή η αποτίμηση της ασφάλειας, είναι η ύπαρξη ενός συνόλου απαιτήσεων που δεν πρέπει για κανένα λόγο να απουσιάζουν ή να αγνοούνται. Τα χαρακτηριστικά που είναι κοινά αποδεκτά είναι :

ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑ (Confidentiality) , που σημαίνει προστασία από το να έχουν πρόσβαση μη εξουσιοδοτημένα λογικά ή φυσικά αντικείμενα (π. χ. προγράμματα, άνθρωποι κ. α.) . Μόνο οι εξουσιοδοτημένοι χρήστες μπορούν να δουν τα προστατευμένα δεδομένα.

ΑΚΕΡΑΙΟΤΗΤΑ (Integrity) , είναι η ιδιότητα των στοιχείων του συστήματος (κυρίως των 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.

Το χαρακτηριστικό της ακεραιότητας είναι πολύ δύσκολο να διευκρινιστεί απόλυτα και αυτό γιατί σημαίνει διαφορετικά πράγματα με διαφορετικά περιεχόμενα. Μερικές από τις έννοιες της ακεραιότητας είναι:

- Ακριβής (precise)
- Ορθός (accurate)
- Τροποποίηση μόνο με αποδεκτούς τρόπους (modified only in acceptable ways)
- Τροποποίηση μόνο από εξουσιοδοτημένους ανθρώπους (modified only by authorised people)
- Τροποποίηση μόνο από εξουσιοδοτημένες διεργασίες (modified only by authorised processes)
- Συνέπεια (consistent)

Στην πραγματικότητα όλες αυτές οι έννοιες χρησιμοποιούνται κοινά.

ΔΙΑΘΕΣΙΜΟΤΗΤΑ (Availability) των πόρων του συστήματος είναι η ιδιότητα των πόρων να καθίστανται αμέσως προσπελάσιμοι από κάθε εξουσιοδοτημένο λογικό ή φυσικό αντικείμενο, που απαιτεί παρόμοια πρόσβαση. Η διαθεσιμότητα αναφέρεται τόσο στα δεδομένα όσο και στις υπηρεσίες που πρέπει να παρέχονται.

Οι προσδοκίες του χαρακτηριστικού της Διαθεσιμότητας περιλαμβάνουν:

- Παρουσία του αντικειμένου και της υπηρεσίας με χρησιμοποιήσιμο τρόπο.
- Ικανότητα χειρισμού των απαιτούμενων πόρων
- Συγκεκριμένος χρόνος αναμονής
- Κατάλληλος χρόνος διάθεσης των πόρων

Σκοπός της Διαθεσιμότητας είναι:

- Δίκαιη κατανομή των πόρων
- Έγκαιρη ανταπόκριση στη διάθεση των δεδομένων
- Ελεγχόμενη συμφωνία, δηλαδή χειρισμός δοσοληψιών, αποκλειστική πρόσβαση, χειρισμός του φαινόμενου deadlock.

• Χρησιμότητα, οι πόροι και τα δεδομένα μπορούν να χρησιμοποιηθούν όπως σχεδιάστηκαν.

Πέρα από τα παραπάνω χαρακτηριστικά στην πράξη υπάρχουν και άλλα, όπως η αυθεντικότητα, η αξιοπιστία, η δυνατότητα ελέγχου κ.α. που πρέπει να λαμβάνονται υπόψιν.

Σε αυτό το σημείο πρέπει να αναφέρουμε ότι η προστασία και η τήρηση όλων των παραπάνω , δηλαδή της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας τους είναι ο στόχος ασφάλειας των **πληροφοριών**[1].

---

[1]*ΜΠΟΖΙΟΣ ΕΛ. (2004) "Σημειώσεις Εφαρμοσμένης Ασφάλειας πληροφοριακών συστημάτων"*

1.3 Βασικές υποθέσεις-παραδοχές

Η ραγδαία αύξηση του ενδιαφέροντος για τα θέματα ασφάλειας είχε ως συνέπεια να υπάρξουν παραδοχές και υποθέσεις, οι οποίες γίνονται σιωπηρά αποδεκτές αν και δεν είναι τόσο αυταπόδεικτες.

Παρακάτω γίνεται μια προσεγγιστική ανάλυση των περισσότερο σημαντικών παραδοχών στην προσπάθεια εξέτασης των θεμάτων ασφάλειας.

Όταν λέμε ασφάλεια εννοούμε την Εμπιστευτικότητα, την Ακεραιότητα και την Διαθεσιμότητα, αλλά και την αξιοπιστία, την δυνατότητα ελέγχου και την αυθεντικότητα.

- Όλοι οι μηχανισμοί ασφάλειας πληροφοριακού συστήματος πρέπει να προστατεύουν όλες τις μορφές πληροφορίας είτε πρόκειται για την αποθήκευση της πληροφορίας σε μαγνητικά μέσα ή την ηλεκτρονική επεξεργασία από τον υπολογιστή , είτε ακόμα για τα έντυπα, τις εικόνες, τα διαγράμματα που υπάρχουν σε ένα σύστημα και που παίζουν σημαντικό ρόλο στην διάδοση της πληροφορίας.
- Η κακομεταχείριση του συστήματος μπορεί να γίνει όχι μόνο από όσους είμαι μέσα σε αυτό, αλλά και από άλλους, όπως είναι οι ανταγωνιστές και γενικά οποιοσδήποτε έχει κάποιο κίνητρο, ικανότητα, γνώσεις και δυνατότητα πρόσβασης στο σύστημα και στους πόρους του.
- Τήρηση της αρχής ότι "κάποιος πρέπει να γνωρίζει μόνο όσα του είναι απαραίτητα για την εκτέλεση της εργασίας του" (need-to-know principle).
- Η υιοθέτηση των μέτρων ασφάλειας ανεξάρτητα από το κόστος τους είναι πολύ βασική, γιατί μπορεί μεν στην πράξη να επιτυγχάνονται λίγες απειλές, ωστόσο οι ζημιές που προκαλούν είναι πολύ μεγάλες και συχνά ανεπανόρθωτες.
- Η ασφάλεια και η προστασία του Π.Σ. είναι υπόθεση πολλών ατόμων (όπως θα εξετασθεί παρακάτω), καθενός από την σκοπιά του και ανάλογα με τις γνώσεις και τις δυνατότητες του.

1.4 Πολιτικές ασφάλειας ενός πληροφοριακού συστήματος

Η διαχείριση ασφάλειας πληροφοριακών συστημάτων στοχεύει στην προστασία των ΠΣ, περιορίζοντας την επικινδυνότητα σε αποδεκτό επίπεδο. Περιλαμβάνει συνοπτικά τις ακόλουθες διαδικασίες :

- Αξιολόγηση της επικινδυνότητας και προσδιορισμό του αποδεκτού επιπέδου ασφάλειας
- Ανάπτυξη και εφαρμογή μιας Πολιτικής Ασφάλειας
- Δημιουργία κατάλληλου οργανωτικού πλαισίου και εξασφάλιση των απαιτούμενων πόρων για την εφαρμογή της πολιτικής ασφάλειας
- Εκπαίδευση, ενημέρωση και ευαισθητοποίηση των χρηστών των ΠΣ

Η πολιτική ασφάλειας των πληροφοριακών συστημάτων περιλαμβάνει το σκοπό και τους στόχους της ασφάλειας , οδηγίες , διαδικασίες, κανόνες, ρόλους και υπευθυνότητες που αφορούν την προστασία των ΠΣ ενός οργανισμού. Η πολιτική ασφάλειας διατυπώνεται σε ένα έγγραφο το οποίο θα πρέπει να γνωρίζουν και να εφαρμόζουν όλοι οι χρήστες των ΠΣ.

Οι οδηγίες και οι διαδικασίες που περιλαμβάνονται στην πολιτική ασφάλειας υλοποιούνται με την μορφή των μέτρων προστασίας ή ασφάλειας(security measures,security controls).

Η πολιτική ασφάλειας μαζί με το σύνολο των μέτρων προστασίας, αποτελούν το σχέδιο ασφάλειας για τα πληροφοριακά συστήματα ενός οργανισμού.

1.4.1 Ο λόγος εφαρμογής Πολιτικών Ασφάλειας

Μια πολιτική ασφάλειας εφαρμόζεται για τους εξής λόγους[2] :

- γιατί χρειαζόμαστε ένα συστηματικό και ολοκληρωμένο πλαίσιο που θα καθοδηγήσει την υλοποίηση των μέτρων ασφάλειας
- γιατί λειτουργεί ως το μέσο για την επικοινωνία των εμπλεκομένων στα ζητήματα ασφάλειας (χρήστες, διοίκηση, διαχειριστές συστημάτων κλπ.)
- γιατί δεν διαθέτουμε απεριόριστους πόρους (χρήματα, χρόνο, ανθρώπινο δυναμικό)
- γιατί έτσι θεμελιώνεται η σημασία της ασφάλειας του ΠΣ για όλα τα μέλη του οργανισμού
- γιατί σε ορισμένες περιπτώσεις αποτελεί νομική υποχρέωση
- γιατί αποτελεί παράγοντα εμπιστοσύνης στις σχέσεις του οργανισμού με συνεργαζόμενους φορείς και πελάτες.

1.4.2 Χαρακτηριστικά Πολιτικών Ασφάλειας

Όταν αναπτύσσουμε μια Πολιτική Ασφάλειας επιδιώκουμε τα ακόλουθα :

- οι οδηγίες και τα μέτρα προστασίας να καλύπτουν το σύνολο των αγαθών του ΠΣ (πληρότητα)
- να λάβουμε υπόψη τις τρέχουσες τεχνολογικές εξελίξεις (επικαιρότητα)
- με κάποιες τροποποιήσεις ή προσθήκες να μπορεί η Πολιτική να καλύπτει μικρές αλλαγές ή επεκτάσεις στο ΠΣ (γενικευσιμότητα)
- η Πολιτική Ασφάλειας στο σύνολο των μελών του οργανισμού και θα πρέπει να είναι εύκολα κατανοητή από όλους (σαφήνεια)
- η περιγραφή των μέτρων ασφάλειας δεν θα πρέπει να δεσμεύει τον οργανισμό σε συγκεκριμένα προϊόντα και τεχνολογίες(τεχνολογική ανεξαρτησία)
- οι απαιτήσεις ασφάλειας πρέπει να καλύπτουν τις ανάγκες του συγκεκριμένου οργανισμού και τέλος (καταλληλότητα)

---

[2]*ΚΑΡΥΔΑ ΜΑΡΙΑ (2010) "Πολιτικές Ασφάλειας Πληροφοριακών Συστημάτων "*

- τα μέτρα προστασίας θα πρέπει να μπορούν να εφαρμοστούν χωρίς να δυσχεραίνουν δυσανάλογα τις δραστηριότητες των χρηστών του ΠΣ (εφαρμοσιμότητα)

Συνοπτικά λοιπόν θα λέγαμε ότι :

- η Πολιτική Ασφάλειας[3] των ΠΣ αποτελεί το βασικό εργαλείο για την διαχείριση ασφάλειας των ΠΣ
- η ανάπτυξη μιας Πολιτικής απαιτεί την καταγραφή σε ένα έγγραφο των βασικών στόχων της ασφάλειας μαζί με τους τρόπου και τα μέσα επίτευξης των στόχων αυτών
- το περιεχόμενο, η μορφή και ο τρόπος εφαρμογής μιας Πολιτικής μπορεί να διαφοροποιηθούν ανάλογα με τον οργανισμό και το ΠΣ
- η αποτελεσματική εφαρμογή της εξαρτάται μεταξύ άλλων, από την υποστήριξη και συμμετοχή της διοίκησης, τη σταδιακή εφαρμογή και την συμβολή της Πολιτικής στην επίτευξη των στόχων του οργανισμού.

[3] *ΚΑΤΣΙΚΑΣ Κ. ΣΩΚΡΑΤΗΣ " Πολιτικές Ασφάλειας Πληροφοριακών Συστημάτων " .*

ΚΕΦΑΛΑΙΟ 2

ΕΝΝΟΙΑ ΤΗΣ ΑΣΦΑΛΕΙΑΣ & ΕΠΙΚΙΝΔΥΝΟΤΗΤΑ ΣΤΑ ΠΣ

2.1 Συγκεκριμενοποίηση της έννοιας της ασφάλειας στα πληροφοριακά συστήματα

Λαμβάνοντας υπόψιν τη νομική άποψη για να δώσουμε τον ορισμό της ασφάλειας θα λέγαμε ότι ασφάλεια είναι η φυσική και νομική κατάσταση κατά την οποία διαπιστώνεται :

- έλλειψη παρόντος κινδύνου
- αποτροπή μελλοντικών κινδύνων
- εξασφάλιση των προστατευόμενων έννομων αγαθών

Σε αυτό είναι απαραίτητο να προσθέσουμε τις εξής γενικές έννοιες που κρίνονται απαραίτητες για την κατανόηση του ορισμού.

- Αγαθό (οτιδήποτε χρήζει προστασίας υλικό ή λογισμικό)
- Ιδιοκτήτης (ο νόμιμος κάτοχος ενός αγαθού)
- Εξουσιοδότηση (παροχή δικαιώματος χρήσης από τον ιδιοκτήτη σε φυσικό πρόσωπο ή διαδικασία)
- Αξία (μέτρο έκφρασης της σπουδαιότητας του αγαθού)
- Επίπτωση (οι συνέπειες που μπορεί να έχει η απώλεια ή βλάβη του αγαθού)
- Αδυναμία (vulnerability)

  -χαρακτηριστικό που είναι δυνατόν να επιτρέψει μια παραβίαση
- Απειλή (threat)

  -παράγων που μπορεί να προξενήσει ζημιά
- Ρήγμα ασφάλειας (breach) ή παραβίαση (violation0

  -συμβάν κατά το οποίο το αγαθό υφίσταται ζημιά
- Μέσο προστασίας (safeguard)

  -ενέργειες και μηχανισμοί για τον περιορισμό των κινδύνων
- Πρόληψη

  -εφαρμογή μέσων προστασίας για να μην συμβεί παραβίαση
- Ανίχνευση

-εντοπισμός ότι έγινε παραβίαση

- Επανόρθωση

  -αποκατάσταση των επιπτώσεων της παραβίασης

- Κόστος

  -σε χρήμα, υποβάθμιση απόδοσης, δυσαρέσκεια

2.2 Η έννοια του κινδύνου σε ένα ΠΣ

Κίνδυνος[4] είναι ότι μπορεί να προκαλέσει ζημιά σε μία ιδιότητα ενός αγαθού. Σχηματικά μπορούμε να το παρουσιάσουμε ως εξής :

(Σχ.2 Παρουσίαση του κινδύνου σε ένα πληροφοριακό σύστημα)

---

[4]*ΚΑΤΣΙΚΑΣ ΣΩΚΡΑΤΗΣ "Πολιτικές και Διαχείριση Ασφάλειας , εισαγωγικά θέματα"*

Ο κίνδυνος σε ένα πληροφοριακό σύστημα μπορεί να αποκαλυφθεί με διάφορους τρόπους. Μία αποκάλυψη είναι ένας τρόπος για πιθανή απώλεια ή βλάβη του πληροφοριακού συστήματος. Παραδείγματα των αποκαλύψεων είναι η μη εξουσιοδοτημένη αποκάλυψη των δεδομένων, τροποποίηση των δεδομένων ή άρνηση του νόμιμου δικαιώματος πρόσβασης στο σύστημα. Η ευπάθεια είναι η αχίλλειος πτέρνα στο σύστημα ασφάλειας που μπορεί να εκμεταλλευτεί από τρίτους για την πρόκληση απωλειών ή ζημίας. Υπάρχουν τέσσερα είδη κινδύνου που απειλούν την ασφάλεια του πληροφοριακού συστήματος που είναι :

- **Η Διακοπή** (**interruption**). Τα αντικείμενα του συστήματος χάνονται, δεν είναι διαθέσιμα ή είναι μη χρησιμοποιήσιμα. Παραδείγματα είναι η ηθελημένη καταστροφή μιας συσκευής, το σβήσιμο ενός προγράμματος ή ενός αρχείου δεδομένων, ή η δυσλειτουργία του διαχειριστή αρχείων του λειτουργικού συστήματος, έτσι ώστε να μην μπορεί να βρεθεί ένα συγκεκριμένο αρχείο στο δίσκο.
- **Η Παρεμπόδιση** (**interception**). Σημαίνει πως μια μη εξουσιοδοτημένη ομάδα έχει κερδίσει το δικαίωμα πρόσβασης σε ένα αντικείμενο. Αυτή η εξωτερική ομάδα μπορεί να είναι είτε πρόσωπα, είτε προγράμματα ή ακόμα και παρέμβαση ενός άλλου πληροφοριακού συστήματος. Παραδείγματα αυτού του είδους της αποτυχίας είναι η παράνομη αντιγραφή των προγραμμάτων ή των αρχείων δεδομένων ή οι υποκλοπές των τηλεφωνημάτων για την απόκτηση δεδομένων από το δίκτυο. Παρόλο που μια απώλεια μπορεί να αποκαλυφθεί σχετικά γρήγορα, ο υποκλοπέας μπορεί να μην αφήσει καθόλου ίχνη για την ανίχνευση της ύπαρξης του.
- Εάν μια μη εξουσιοδοτημένη ομάδα όχι μόνο προσπελάσει τα δεδομένα, αλλά ανακατευτεί και με κάποια αντικείμενα, τότε μιλάμε για **τροποποίηση** (**modification**). Για παράδειγμα κάποιος μπορεί να αλλάξει τις τιμές σε μια βάση δεδομένων ή να μετατρέψει ένα πρόγραμμα έτσι ώστε να εκτελεί επιπλέον υπολογισμούς ή να τροποποιεί τα δεδομένα που μεταφέρονται ηλεκτρονικά. Είναι ακόμα δυνατό να τροποποιηθεί και το υλικό μέρος του συστήματος.

- Τέλος μια μη εξουσιοδοτημένη ομάδα μπορεί να **κατασκευάσει** (**fabricate**) πλαστά αντικείμενα σε ένα Π.Σ. Ο εισβολέας μπορεί να προσθέσει εγγραφές σε μια υπάρχουσα βάση δεδομένων. Μερικές φορές αυτές οι προσθέσεις ανιχνεύονται σαν πλαστές, αλλά εάν έχουν γίνει περίτεχνα τότε είναι αδιαχώριστες από τα πραγματικά αντικείμενα.

2.3 Απώλειες που μπορεί να προκληθούν από την εκδήλωση ενός κινδύνου

Οι απώλειες που μπορούν να συμβούν σε ένα Π.Σ. μπορούν να ταξινομηθούν σε τρεις κατηγορίες :

α) **Αδυναμία Χρήσης του Η/Υ**. Δηλαδή, όταν ο Η/Υ είναι εκτός ενέργειας, οι υπηρεσίες που παρέχει διακόπτονται, αυτό μπορεί να οφείλεται:

i) Προσωρινή Διακοπή εξαιτίας πτώσης του ηλεκτρικού ρεύματος. Η αντιμετώπιση γίνεται με γεννήτριες παροχής ηλεκτρικού ρεύματος, οι οποίες συνδέονται αυτόματα στο δίκτυο αν και όταν παραστεί ανάγκη (UPS, Uninterrupted Power Supply) .

ii) Αδυναμία Σύνδεσης με τον κεντρικό Η/Υ εξαιτίας υπερφόρτωσης των τηλεπικοινωνιακών δικτύων ή εξαιτίας της μειωμένης αξιοπιστίας του δικτύου. Το πρόβλημα αυτό είναι ιδιαίτερα σοβαρό σε αποκεντρωμένα Π.Σ. που λειτουργούν όμως με συγκεντρωτική μέθοδο επεξεργασίας (π.χ. δίκτυα Τραπεζών) .

iii) Πρόβλημα Υλικού, εξαιτίας ανθρώπινου λάθους ή πλημμελούς συντήρησης.

iv) Πρόβλημα Λογισμικού, εξαιτίας ανθρώπινου λάθους ή επαγγελματικής ανεπάρκειας. Σε ότι αφορά την προμήθεια τυποποιημένων εφαρμογών, η πιο καλή αντιμετώπιση είναι η εγγύηση διαρκούς καλής λειτουργίας και ο μακρύς

χρόνος παράλληλης λειτουργίας της νέας εφαρμογής με το χειρόγραφο ή αυτοματοποιημένο σύστημα που αντικατέστησε.

β) **Απώλεια Χρημάτων**. Αν το Π.Σ. καταστραφεί ή η λειτουργία του υποβαθμισθεί, τότε υπάρχει απώλεια χρημάτων και μπορεί να εμφανισθεί σε δυο μορφές.

i) Χρήση του Η/Υ. Δηλαδή στελέχη ενός Κέντρου Πληροφορικής να χρησιμοποιούν τις δυνατότητες που τους παρέχονται για έργο διαφορετικό από αυτό που τους ανατέθηκε.
ii) Κλοπή του Η/Υ. Συνήθως πρόκειται για μεσαία και μεγάλα συστήματα.

γ) **Απώλεια Αποκλειστικής Χρήσης**. Αν ένας μη εξουσιοδοτημένος χρήστης μπορέσει να χρησιμοποιήσει το Π.Σ., τότε ο κάτοχος του παύει να έχει την αποκλειστική του χρήση.

Οι παραπάνω απώλειες[5] μπορούν να διαχωριστούν και σε άλλες δυο ομάδες:

i) ***ΗΘΕΛΗΜΕΝΕΣ,*** δηλαδή όταν ο μη εξουσιοδοτημένος χρήστης έχει σαφή γνώση των αποτελεσμάτων των ενεργειών του.
ii) ***ΑΘΕΛΗΤΕΣ***, όταν δηλαδή ο μη εξουσιοδοτημένος χρήστης δεν έχει επίγνωση των αποτελεσμάτων των ενεργειών του.

---

[5]*ΜΠΟΖΙΟΣ ΕΛ. (2004) "Σημειώσεις Εφαρμοσμένης Ασφάλειας Πληροφοριακών Συστημάτων"*

2.4 Επικινδυνότητα και συναφείς έννοιες

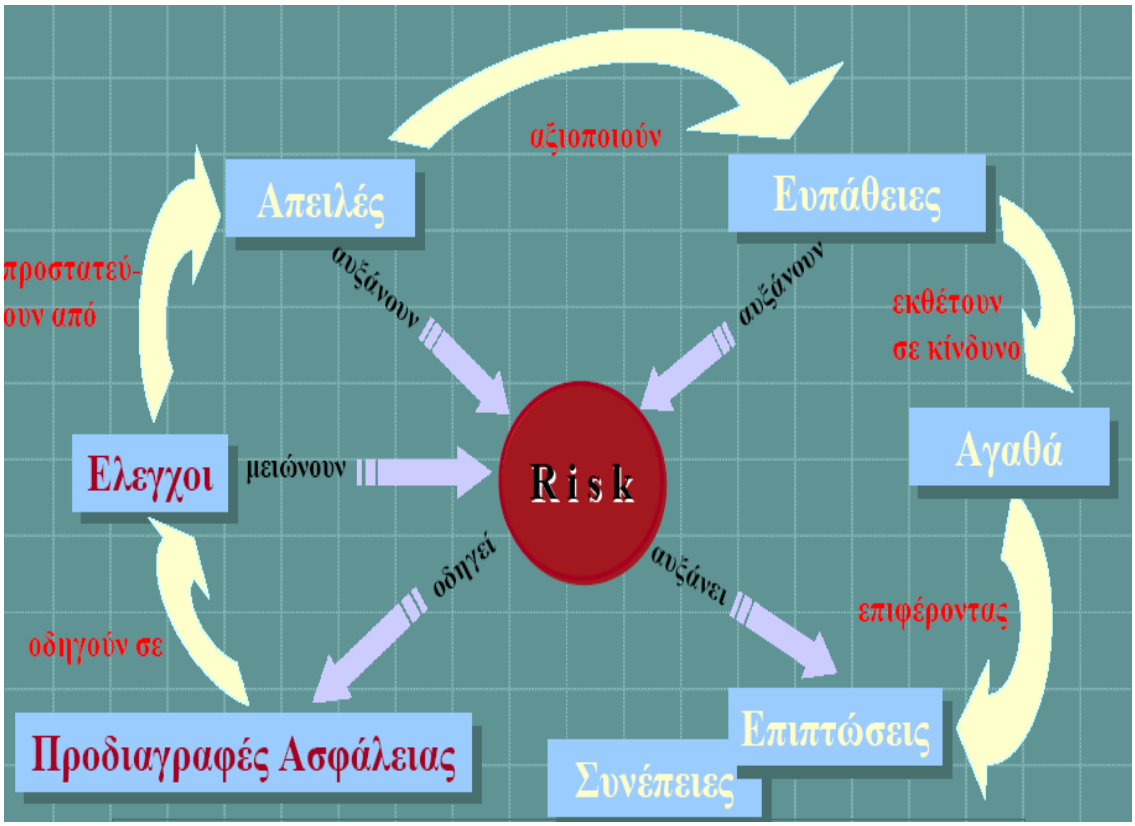
Η ανάλυση επικινδυνότητας (risk analysis) απαντά στο ερώτημα της επιλογής αντιμέτρων που θα προσφέρουν προστασία *ανάλογη* των κινδύνων που απειλούν το ΠΣ. Η ανάλυση επικινδυνότητας αναστρέφει το μοντέλο της *αξιολόγησης επενδύσεων*, όπου μία επένδυση θεωρείται συμφέρουσα αν το κόστος της (σε σταθερές τιμές) υπολείπεται του γινομένου του αναμενόμενου κέρδους επί την πιθανότητα επίτευξης του κέρδους. Εδώ, η *επικινδυνότητα* (Ε) ορίζεται ως το γινόμενο της *πιθανότητας* (Π) πραγματοποίησης ενός επεισοδίου ασφάλειας (security incident) επί το *κόστος* (Κ) που θα επιφέρει το επεισόδιο ασφάλειας, ήτοι: $Ε = Π \times Κ$.

Αναλυτικότερα, η πιθανότητα πραγματοποίησης ενός επεισοδίου εκτιμάται ως συνάρτηση της πιθανότητας εμφάνισης μίας ***απειλής*** (threat) και της σχετικής ***ευπάθειας*** (αδυναμία, αλωσιμότητα, vulnerability) του συστήματος που δύναται να επιτρέψει στην απειλή να πραγματοποιηθεί. Αντίστοιχα, το κόστος από την πραγματοποίηση ενός επεισοδίου εκτιμάται με βάση την ***επίπτωση*** (impact) πάνω στον οργανισμό, που θα έχει η ζημιά που θα προκληθεί στα ***περιουσιακά στοιχεία*** (*αγαθά*, assets) του ΠΣ. Έτσι, τελικά, η επικινδυνότητα εκτιμάται ως συνάρτηση τριών παραγόντων: (α) της αξίας των *αγαθών* (assets), που προκύπτει από την αντίστοιχη επίπτωση της ζημιάς που θα υποστούν, (β) της σοβαρότητας των *απειλών* (threats) και (γ) του επιπέδου της *ευπάθειας* (vulnerability) του ΠΣ.

Το μοντέλο αυτό δίνει τη δυνατότητα αποτίμησης της επικινδυνότητας σε χρηματικούς όρους, έτσι ώστε να συγκριθεί με το κόστος των σχετικών αντιμέτρων. Συχνότερα, όμως, η αποτίμηση γίνεται σε απλή αριθμητική κλίμακα, καθώς οι επιπτώσεις από την απώλεια ορισμένων αγαθών (π.χ. απώλεια ανθρώπινης ζωής) είναι δύσκολο να αποτιμηθούν οικονομικά.

Η ανάλυση της επικινδυνότητας αποτελεί προϋπόθεση για τη μετέπειτα διαχείρισής της, που είναι και ο αντικειμενικός στόχος της όλης προσπάθειας. Ο όρος *διαχείριση επικινδυνότητας* αναφέρεται στον έλεγχο της επικινδυνότητας, ώστε να παραμένει σε αποδεκτά επίπεδα. Η επικινδυνότητα μπορεί να μειωθεί, με την εφαρμογή αντιμέτρων,

να μεταβιβαστεί, π.χ. με ασφάλιση, ή να αναληφθεί, δηλαδή να αποδεχθούμε ότι είμαστε διατεθειμένοι να υποστούμε τις επιπτώσεις αν συμβεί ένα επεισόδιο[6].



(Σχ.3Επικινδυνότητα πληροφοριακού συστήματος σχηματικά. Πηγή: Δ. *Γκρίτζαλης, Αυτονομία και Πολιτική Ανυπακοή στον Κυβερνοχώρο, Παπασωτηρίου, Αθήνα 2004.)*

[6]*ΚΟΚΟΛΑΚΗΣ ΣΠ. "Ανάλυση , αποτίμηση και διαχείριση επικινδυνότητας ΠΣ"*

Συνοπτικά λοιπόν , η επικινδυνότητα είναι συνάρτηση :

- της αξίας των αγαθών (A, Asset)
- του βαθμού των ευπαθειών (V, Vulnerability)
- της πιθανότητας εμφάνισης (T, Threat)
- της έντασης των επιπτώσεων που θα έχουν οι απειλές αν πραγματοποιηθούν (I , Impact)

$$R = f (A , V , T , I)$$

Διαγραμματικά θα αναφέρουμε και κάποιες επιπλέον έννοιες με την επικινδυνότητα που όμως είναι σημαντικές για περαιτέρω κατανόηση της.

Ανάλυση

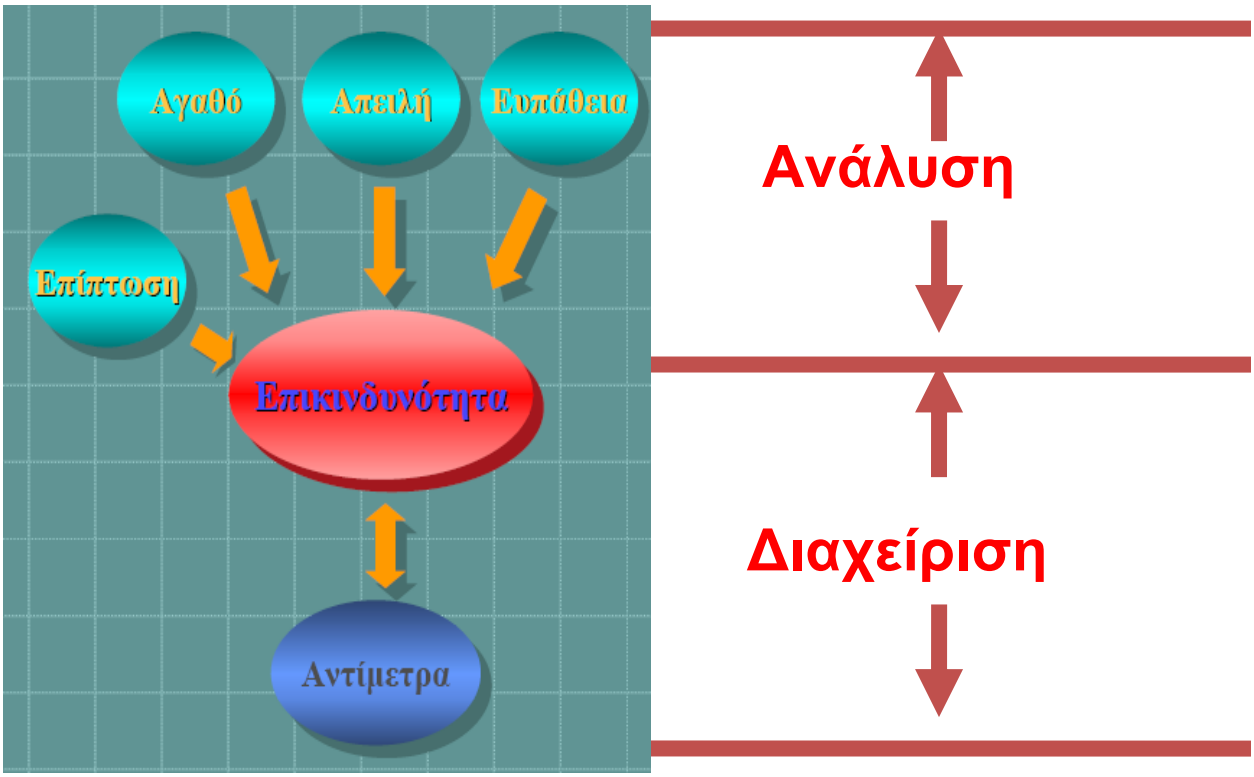
- Καταγραφή πόρων (assets)
- Αξιολόγηση απειλών (threats)
- Εξέταση αδυναμιών (vulnerabilities) ή ευπαθειών
- Ορισμός επιπτώσεων
    - Ποσοτικός / ποιοτικός προσδιορισμός επιπτώσεων
- Προσδιορισμός μεθόδων προστασίας (Countermeasure/safeguard – αντίμετρο)
    - Προληπτικοί / Κατασταλτικοί
- Κοστολόγηση
    - Χρήμα
    - Φήμη

Διαχείριση

- Συνεχής παρακολούθηση, εξέταση, έλεγχος
    - παρακολούθηση και βελτίωση
    - προσαρμογή σε νέες ανάγκες και απειλές

- Περιορισμός της επικινδυνότητας σε αποδεκτά επίπεδα
  - ✓ Μείωση επικινδυνότητας, π.χ. υιοθέτηση νέου αντιμέτρου
  - ✓ Μεταβίβαση επικινδυνότητας σε τρίτους, π.χ. Ασφάλιση
  - ✓ Αποδοχή επικινδυνότητας

- Στάδια:
  - ✓ Επιλογή αντιμέτρων.
  - ✓ Καθορισμός πολιτικής ασφάλειας.
  - ✓ Σύνταξη σχεδίου ασφάλειας.
  - ✓ Εφαρμογή και παρακολούθηση του σχεδίου ασφάλειας[7]



(Σχ.4 Φάσεις ανάλυσης και διαχείρισης επικινδυνότητας)

---

[7] *Δρ.ΠΑΠΑΝΑΓΙΩΤΟΥ ΚΩΝ..2009 "Προστασία και ασφάλεια υπολογιστικών συστημάτων"*

ΚΕΦΑΛΑΙΟ 3

Η ΜΕΘΟΔΟΛΟΓΙΑ ΤΗΣ ΑΝΑΛΥΣΗΣ & ΔΙΑΧΕΙΡΙΣΗΣ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ

Με τον όρο *μεθοδολογία* εννοούμε ένα οργανωμένο σύνολο αρχών και κανόνων, το οποίο καθοδηγεί τη δράση σ' ένα συγκεκριμένο γνωστικό χώρο. Μεθοδολογία είναι ο *λόγος περί της μεθόδου*. Προδιαγράφει, δηλαδή, τις μεθόδους που μπορούν να χρησιμοποιηθούν σ' ένα γνωστικό χώρο, εκφράζοντας με αυτόν τον τρόπο μία συγκεκριμένη άποψη (φιλοσοφική, επιστημολογική, βιωματική). Η μεθοδολογία "υλοποιείται" με ένα σύνολο *μεθόδων, τεχνικών* και *εργαλείων*. Η μεθοδολογία της *ανάλυσης και διαχείρισης επικινδυνότητας ΠΣ* υιοθετεί τις βασικές αρχές και το επιστημολογικό υπόβαθρο της στατιστικής επιστήμης και των πιθανοτήτων και κυρίως του κλάδου που αναφέρεται συνήθως ως στατιστική Bayes (Bayesian Statistics), από το όνομα του μαθηματικού Thomas Bayes (1702-1761) που διατύπωσε το ομώνυμο θεώρημα. Η περιγραφή του θεωρήματος βρίσκεται εκτός των στόχων της παρούσας εργασίας.

3.1 Πλεονεκτήματα και μειονεκτήματα

Στα πλεονεκτήματα της ανάλυσης και διαχείρισης επικινδυνότητας περιλαμβάνονται τα παρακάτω:

- Δίνει τη δυνατότητα αιτιολόγησης του κόστους των αντιμέτρων.
- Αποτελεί ένα εργαλείο επικοινωνίας ανάμεσα στους ειδικούς των ΠΣ και τη διοίκηση των οργανισμών, καθώς επιτρέπει την έκφραση του προβλήματος της ασφάλειας σε γλώσσα κατανοητή από τη διοίκηση, αντιμετωπίζοντας την ασφάλεια ως ‘επένδυση’ που αποτιμάται με όρους κόστους/οφέλους.

- Είναι αρκετά ευέλικτη, ώστε να μπορεί να ενταχθεί σε διάφορα επιστημολογικά πλαίσια και να εφαρμόζεται είτε αυτούσια, είτε σε συνδυασμό με άλλες μεθοδολογίες.
- Καλύπτει τις απαιτήσεις της ευρωπαϊκής και ελληνικής νομοθεσίας, που απαιτούν από τα ΠΣ, τα οποία επεξεργάζονται προσωπικά δεδομένα, τη λήψη μέτρων προστασίας, έτσι ώστε "να εξασφαλίζεται επίπεδο ασφάλειας ανάλογο προς τους κινδύνους που συνεπάγεται η επεξεργασία και η φύση των δεδομένων" (Νόμος 2472/1997, άρθρο 10, παρ. 3,)[8].
- Διευκολύνει την καλύτερη κατανόηση της φύσης και της λειτουργίας του πληροφοριακού συστήματος. Αποτελεί, δηλαδή, ένα μέσο τεκμηρίωσης και ανάλυσης του πληροφοριακού συστήματος.
- Αποτελεί την πλέον διαδεδομένη μεθοδολογία[9] σχεδιασμού και διαχείρισης της ασφάλειας ΠΣ και έχει εφαρμοστεί με επιτυχία σε ένα μεγάλο πλήθος περιπτώσεων.

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

- Στηρίζεται σε ένα απλοϊκό μοντέλο του ΠΣ και αγνοεί τα ιδιαίτερα χαρακτηριστικά και τις απαιτήσεις του οργανισμού στον οποίο ανήκει το ΠΣ.
- Εμπεριέχει σημαντική υποκειμενικότητα στις εκτιμήσεις τόσο της αξίας των αγαθών (assets), όσο και στην αποτίμηση απειλών (threats) και ευπάθειας (vulnerability). Η υποκειμενικότητα αυτή συχνά συγκαλύπτεται πίσω από την αυστηρότητα των μαθηματικών-πιθανοτικών μοντέλων, στα οποία στηρίζεται, τη συστηματικότητα των περισσότερων μεθόδων ανάλυσης επικινδυνότητας και την ‘αντικειμενικότητα’ των εργαλείων που υποστηρίζουν τις σχετικές μεθόδους.
- Βασίζεται σε απλές στατιστικές μεθόδους για τον υπολογισμό της πιθανότητας εμφάνισης μιας απειλής. Η εγκυρότητα της εφαρμογής των μεθόδων αυτών στον τομέα της ασφάλειας πληροφοριακών συστημάτων έχει αμφισβητηθεί από πολλούς ερευνητές.

---

[8] *ΝΟΜΟΣ 2472/97, “Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα”10-4-1997/ΦΕΚ 50/Τεύχος Α', 1997.*

[9]*ΚΟΚΟΛΑΚΗΣ ΣΠ.. “Ανάλυση , αποτίμηση και διαχείριση επικινδυνότητας ΠΣ.*

3.2 Μέθοδοι ανάλυσης και διαχείρισης επικινδυνότητας

Όπως προαναφέρθηκε, μία μεθοδολογία δίνει το πλαίσιο, εντός του οποίου αναπτύσσονται και εφαρμόζονται μία ή περισσότερες μέθοδοι. Μέθοδος είναι "ο συστηματικός και προγραμματισμένος τρόπος προσεγγίσεως, εξετάσεως, αναλύσεως και ερμηνείας προβλημάτων ή φαινομένων βάσει συγκεκριμένων κανόνων…". Με άλλα λόγια, μέθοδος είναι ένας κανονικός και συστηματικός τρόπος για να εκτελεστεί ένα έργο.

Έτσι, ένα μεγάλο πλήθος - περισσότερες από εκατό - μεθόδων ανάλυσης και διαχείρισης επικινδυνότητας ΠΣ έχουν αναπτυχθεί, πολλές από τις οποίες υποστηρίζονται από εργαλεία λογισμικού (software tools). Στις παραγράφους που ακολουθούν θα περιγράψουμε ενδεικτικά κάποιες από τις πιο δημοφιλείς μεθόδους καθώς και από τα λογισμικά ανάλυσης κινδύνου.

3.2.1 Μέθοδος OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)

Η μέθοδος OCTAVE αναπτύχθηκε στο συντονιστικό κέντρο CERT (www.cert.org). Η OCTAVE είναι μια αυτό-διευθυνόμενη (self-directed) μέθοδος για ανάλυση κινδύνων. Αυτό σημαίνει ότι το ίδιο το προσωπικό του οργανισμού αναλαμβάνει να διεκπεραιώσει την ανάλυση και να θέσει την στρατηγική ασφαλείας που θα ακολουθηθεί (όπως άλλωστε και στις περισσότερες σύγχρονες ποιοτικές μεθόδους). Η τεχνική αυτή βελτιώνει την γνώση του προσωπικού για τα θέματα και τις πρακτικές ασφαλείας του οργανισμού και πετυχαίνει πιο εύκολη αποδοχή και αφομοίωση των μέτρων αντιμετώπισης που τελικά επιλέγονται.

Όπως δηλώνει και το όνομα, η μέθοδος επικεντρώνεται στα σημεία εκείνα που έχουν άμεση επίδραση στην λειτουργικότητα του οργανισμού και δεν αναλώνεται σε καθαρά τεχνικά θέματα ασφαλείας που δεν εξυπηρετούν τον οργανισμό. Έτσι, αναλύει τις

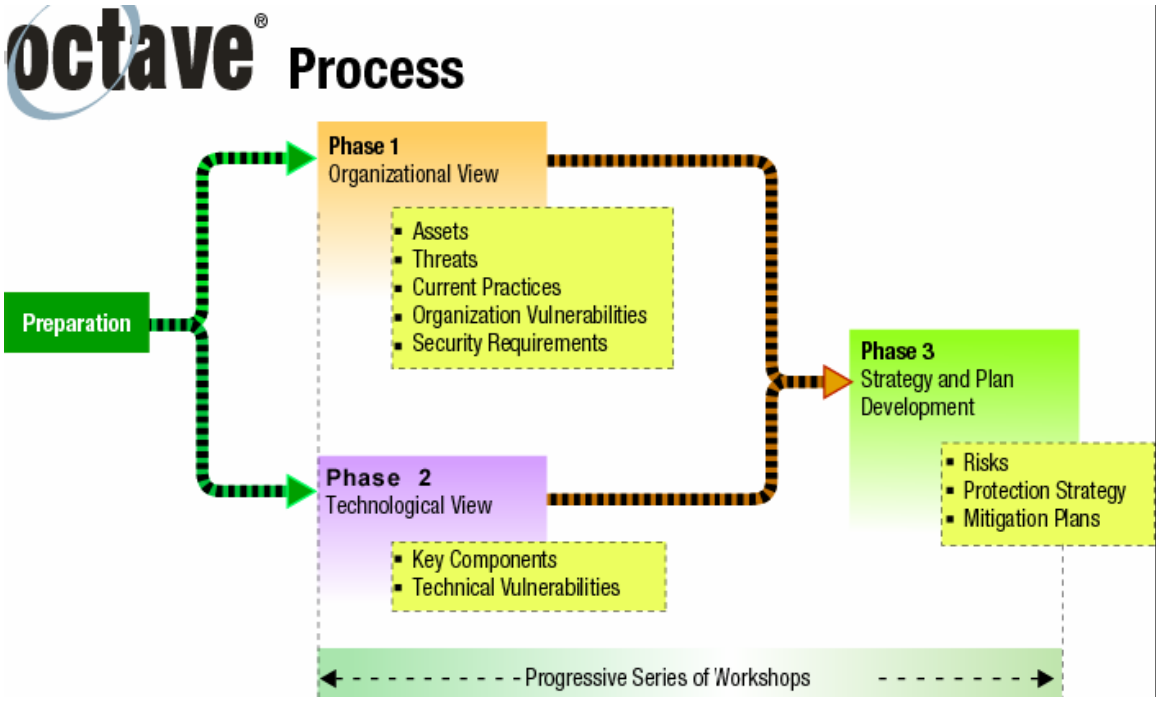
απειλές και ευπάθειες στα περιουσιακά στοιχεία του οργανισμού που έχουν αναγνωριστεί ως τα πιο σημαντικά.

Η μέθοδος αυτή απευθύνεται σε μεγάλους οργανισμούς με προσωπικό 200 ατόμων και πάνω. Για μικρότερους οργανισμούς είναι υπό ανάπτυξη η μέθοδος OCTAVE-S στο CERT, αλλά ακόμα δεν έχει ολοκληρωθεί.

Περιγραφή της μεθόδου

Η μέθοδος OCTAVE ολοκληρώνεται σε 3 φάσεις, κατά τις οποίες εξετάζονται τα οργανωτικά και τα τεχνικά θέματα ασφαλείας ώστε να δημιουργηθεί μια πλήρης εικόνα των αναγκών ασφαλείας του οργανισμού. Η μέθοδος αποτελείται από μια προοδευτική σειρά συσκέψεων (workshops), οι οποίες απαιτούν την ενεργή συμμετοχή όλων των συμμετεχόντων.

Παρακάτω φαίνεται το γενικό σχεδιάγραμμα της μεθόδου.



(Σχ.5 Φάση προετοιμασίας της μεθόδου)

Συσκέψεις OCTAVE

Η μέθοδος OCTAVE περιλαμβάνει συσκέψεις δύο ειδών:

1. Καθοδηγούμενες συζητήσεις μεταξύ των μελών του οργανισμού
2. Συσκέψεις της ομάδας ανάλυσης κινδύνων

Όλες οι συσκέψεις έχουν ένα πρόεδρο και ένα γραμματέα. Ο πρόεδρος είναι υπεύθυνος για την καθοδήγηση όλων των δραστηριοτήτων και για την εξασφάλιση της ολοκλήρωσης τους.

Επίσης πρέπει να διασφαλίζει ότι όλοι οι συμμετέχοντες κατανοούν τους ρόλους τους και ότι οποιοδήποτε νέο ή πρόσθετο μέλος της ομάδας είναι έτοιμο να συμμετέχει ενεργά. Ο γραμματέας καταγράφει όλες τις πληροφορίες που παράγονται κατά την διάρκεια της σύσκεψης, είτε σε γραπτή είτε σε ηλεκτρονική μορφή. Σημειώνεται ότι δεν είναι απαραίτητο ο πρόεδρος ή ο γραμματέας να είναι ο ίδιος σε κάθε σύσκεψη. Για παράδειγμα, ένας πρόεδρος με μεγαλύτερη οργανωτική ικανότητα ταιριάζει καλύτερα στις συσκέψεις της πρώτης φάσης, ενώ ένας πρόεδρος με ικανότητα ανάλυσης και σχεδίασης ταιριάζει περισσότερο στις συσκέψεις την τρίτης φάσης.

Προετοιμασία (Preparation)

Πριν ξεκινήσει η πρώτη φάση της μεθόδου είναι απαραίτητο να γίνει μια προετοιμασία. Μια σωστή προετοιμασία περιλαμβάνει τα εξής:

***Εξασφάλιση υποστήριξης από την διεύθυνση του οργανισμού*:** Αυτός είναι ο πιο σημαντικός παράγοντας για την επιτυχία της ανάλυσης κινδύνων. Αν δεν υπάρχει υποστήριξη τότε το ενδιαφέρον του προσωπικού για την ανάλυση θα χαθεί πολύ γρήγορα. Η συμμετοχή της διεύθυνσης στην διαδικασία εξασφαλίζει επίσης την καλύτερη κατανόηση των κινδύνων από τα προβλήματα ασφαλείας.

***Επιλογή της ομάδας ανάλυσης*:** Η ομάδα είναι υπεύθυνη για την διαχείριση της διαδικασίας και την ανάλυση των πληροφοριών. Τα μέλη της ομάδας πρέπει να έχουν επαρκείς γνώσεις και εκπαίδευση ώστε να μπορούν να ηγηθούν της διαδικασίας. Επιπρόσθετα, πρέπει να είναι σε θέση να γνωρίζουν πότε πρέπει να εμπλουτίζουν την ομάδα με άτομα που έχουν ειδικές γνώσεις αν αυτό απαιτείται.

***Αντικείμενο και εμβέλεια της ανάλυσης*:** Όπως αναφέρθηκε και στις άλλες μεθόδους, η εμβέλεια της ανάλυσης πρέπει να περιλαμβάνει τα σημαντικά μέρη του πληροφοριακού

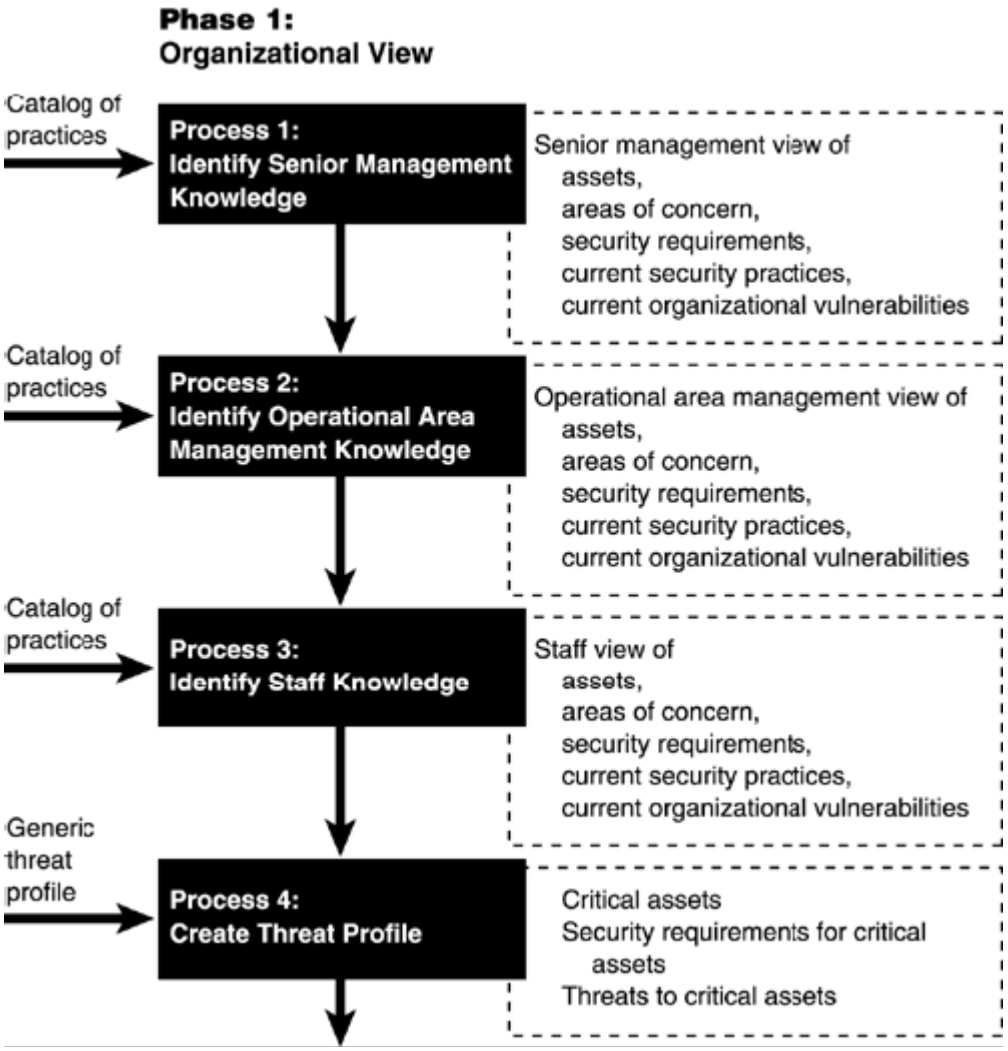
συστήματος χωρίς να ξεφεύγει σε εύρος. Αν το εύρος της ανάλυσης είναι πολύ μεγάλο θα είναι πολύ δύσκολο για την ομάδα να αναλύσει όλα τα δεδομένα. Αν είναι πολύ μικρό τότε τα αποτελέσματα μπορεί να μην είναι τόσο χρήσιμα όσο θα έπρεπε.

***Επιλογή των συμμετεχόντων*:** Κατά την διάρκεια εξαγωγής πληροφοριών της πρώτης φάσης της μεθόδου, μέλη του προσωπικού από διάφορα τμήματα του οργανισμού θα προσφέρουν τις γνώσεις και τις απόψεις τους για τον οργανισμό. Πρέπει να επιλεχθούν για τις συσκέψεις με βάση την εμπειρία, τις γνώσεις και τις ικανότητές τους.

***Οργάνωση των συσκέψεων*:** Καθορισμός των χώρων, του χρονοδιαγράμματος, των υλικών που θα χρειαστούν κτλ.

Φάση 1η

Στην πρώτη φάση αναλύεται η οργανωτική άποψη του οργανισμού με την βοήθεια των ανθρώπων που δουλεύουν σε αυτόν. Η πρώτη φάση μπορεί να χωριστεί σε τέσσερις διαδικασίες όπως φαίνεται στο παρακάτω σχήμα:



(Σχ.6 Προγραμματισμός 1ης φάσης της μεθόδου)

(Πηγή: Managing Information Security Risks: The OCTAVE(SM) Approach)

Διαδικασίες 1-3:

Η ομάδα ανάλυσης οργανώνει συσκέψεις για την απόσπαση πληροφοριών. Συμμετέχοντες από όλο τον οργανισμό συνεισφέρουν τις προσωπικές τους απόψεις για το ποια περιουσιακά στοιχεία (assets) είναι πιο σημαντικά και πόσο πρέπει να προστατευτούν.

Τέσσερις δραστηριότητες ολοκληρώνονται για την απόσπαση πληροφοριών:

1. Αναγνώριση περιουσιακών στοιχείων και σχετικών προτεραιοτήτων
2. Εντοπισμός σημείων ανησυχίας
3. Προσδιορισμός απαιτήσεων ασφαλείας για τα σημαντικότερα περιουσιακά στοιχεία
4. Αποτύπωση γνώσης των υπαρχόντων πρακτικών ασφαλείας και οργανωτικών ευπαθειών

Η επόμενη λίστα δείχνει το ακροατήριο της κάθε διαδικασίας:

1. ***Γενική διεύθυνση***: Στην διαδικασία αυτή συμμετέχουν οι γενικοί διευθυντές του οργανισμού
2. ***Διευθυντές επιμέρους τμημάτων***: Στην διαδικασία αυτή συμμετέχουν οι διευθυντές τμημάτων του οργανισμού
3. ***Προσωπικό***: Στην διαδικασία αυτή συμμετέχει το προσωπικό του οργανισμού. Τα μέλη του προσωπικού που σχετίζονται με την πληροφορική συνήθως συμμετέχουν σε διαφορετική σύσκεψη από ότι τα κανονικά μέλη του προσωπικού

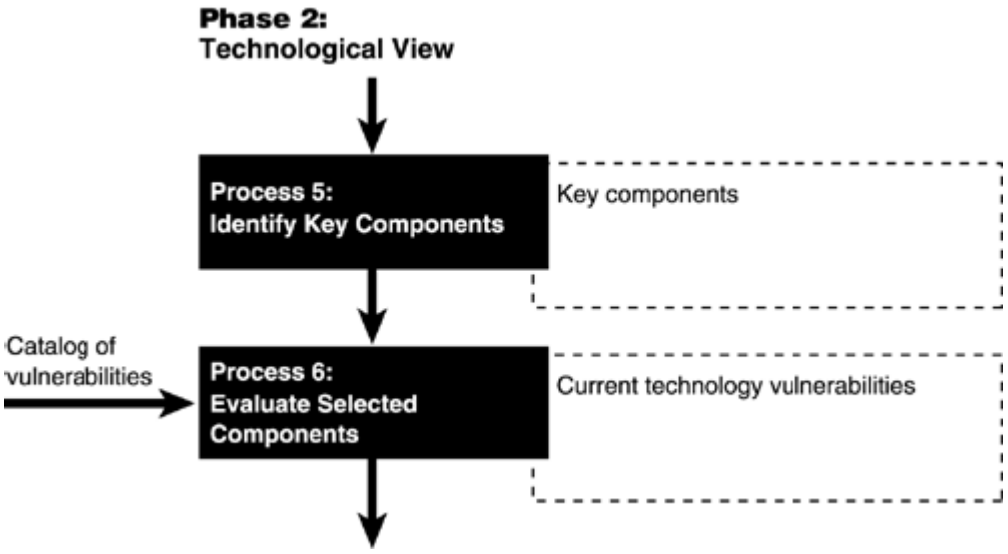
Διαδικασία 4: Δημιουργία προφίλ απειλών

Στην διαδικασία αυτή λαμβάνουν μέρος μόνο τα μέλη της ομάδας ανάλυσης. Κατά την διάρκεια της ανάλυσης η ομάδα αναγνωρίζει τα περιουσιακά στοιχεία που είναι πιο κρίσιμα για τον οργανισμό και περιγράφει με ποιόν τρόπο απειλούνται. Η διαδικασία περιλαμβάνει τα εξής:

- Ενοποίηση των πληροφοριών που συλλέχτηκαν κατά τις 3 πρώτες διαδικασίες
- Επιλογή των πιο κρίσιμων περιουσιακών στοιχείων
- Επανεξέταση και βελτίωση των απαιτήσεων ασφαλείας για τα κρίσιμα περιουσιακά στοιχεία
- Αναγνώριση των απειλών προς τα κρίσιμα περιουσιακά στοιχεία

Φάση 2η

Η δεύτερη φάση της μεθόδου OCTAVE ονομάζεται και τεχνολογική άποψη διότι επικεντρώνεται στην τεχνολογική (υλική) υποδομή του πληροφοριακού συστήματος (συστήματα, υπολογιστές, προγράμματα κτλ). Η δεύτερη φάση περιλαμβάνει 2 διαδικασίες οι οποίες φαίνονται και στο παρακάτω σχεδιάγραμμα:



(Σχ.7 Προγραμματισμός 2ης φάσης της μεθόδου)

(Πηγή: Managing Information Security Risks: The OCTAVE(SM) Approach)

Διαδικασία 5: Αναγνώριση των κρίσιμων συστημάτων

Συμμετέχοντες σε αυτή την διαδικασία είναι η ομάδα ανάλυσης και επιλεγμένα μέλη του προσωπικού πληροφορικής. Σκοπός της διαδικασίας είναι η επιλογή των συστημάτων εκείνων του πληροφοριακού συστήματος του οργανισμού που είναι πιο κρίσιμα, ώστε να αναλυθούν αργότερα ως προς τις ευπάθειες τους. Η διαδικασία 5 περιλαμβάνει δύο δραστηριότητες:

- Αναγνώριση των κρισιμότερων κατηγοριών συστημάτων
- Αναγνώριση των συγκεκριμένων συστημάτων που θα εξεταστούν

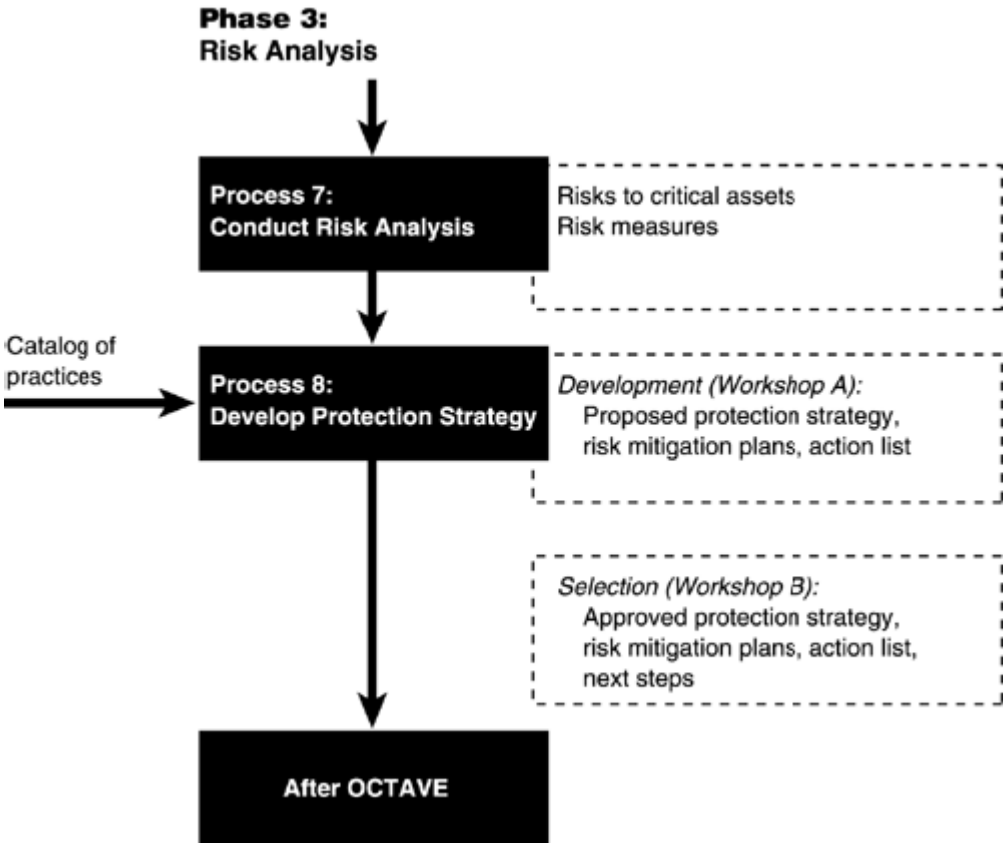
Διαδικασία 6: Εξέταση επιλεγμένων συστημάτων

Συμμετέχοντες σε αυτή την διαδικασία είναι η ομάδα ανάλυσης και επιλεγμένα μέλη του προσωπικού πληροφορικής. Σκοπός της διαδικασίας είναι η αναγνώριση των ευπαθειών στα συστήματα του πληροφοριακού συστήματος που επιλέχθηκαν κατά την διαδικασία 5. Ο βαθμός της ευπάθειας που θα βρεθεί είναι ενδεικτικός της συνολικής ευπάθειας του πληροφοριακού συστήματος του οργανισμού. Κατά την διαδικασία 6 γίνονται τα εξής:

- Εκτέλεση εργαλείων αποτίμησης της ευπάθειας στα επιλεγμένα συστήματα
-Ανασκόπηση των τεχνολογικών ευπαθειών και συγκέντρωση των αποτελεσμάτων

Φάση 3η

Η τρίτη φάση είναι η φάση αντιμετώπισης των κινδύνων που έχουν ανιχνευθεί μέχρι τώρα. Κατά την διάρκεια αυτής της φάσης σχηματίζονται στρατηγικές ασφαλείας και σχέδια αντιμετώπισης των κινδύνων του οργανισμού. Η φάση αυτή αποτελείται από δύο διαδικασίες που φαίνονται στο παρακάτω σχεδιάγραμμα:



(Σχ.8 Προγραμματισμός 3ης φάσης της μεθόδου)

(Πηγή: Managing Information Security Risks: The OCTAVE(SM) Approach)

Διαδικασία 7: Ανάλυση Κινδύνων

Στην διαδικασία αυτή συμμετέχει μόνο η ομάδα ανάλυσης. Σκοπός είναι ο υπολογισμός των κινδύνων στα κρίσιμα περιουσιακά στοιχεία του οργανισμού. Η διαδικασία 7 περιλαμβάνει τα εξής:

- Αναγνώριση και δημιουργία λεπτομερούς περιγραφής του τύπου του αντίκτυπου των απειλών στα κρίσιμα περιουσιακά στοιχεία
- Δημιουργία κριτηρίων για την αποτίμηση των κινδύνων ανάλογα με τις ιδιαίτερες ανάγκες του οργανισμού
- Αποτίμηση του αντίκτυπου των απειλών στα κρίσιμα περιουσιακά στοιχεία

Διαδικασία 8: Σχεδίαση Στρατηγικής Προστασίας

Η διαδικασία 8 περιλαμβάνει 2 συσκέψεις. Στην πρώτη σύσκεψη συμμετέχει η ομάδα ανάλυσης και επιλεγμένα άτομα του οργανισμού που μπορούν να βοηθήσουν στην ανάπτυξη στρατηγικής προστασίας. Σκοπός της διαδικασίας είναι η ανάπτυξη στρατηγικής προστασίας, σχεδίων μείωσης των κινδύνων στα κρίσιμα περιουσιακά στοιχεία και σχεδίου δράσης. Τα βήματα που ακολουθούνται είναι τα εξής:

- Συγκέντρωση των πληροφοριών που συλλέχτηκαν κατά τις διαδικασίες 1-3
-Ανασκόπηση των πληροφοριών του κινδύνου που υπολογίστηκαν κατά την διαδικασία 7
- Δημιουργία στρατηγικής προστασίας
- Δημιουργία σχεδίων μείωσης του κινδύνου
- Δημιουργία σχεδίου δράσης

Στην δεύτερη σύσκεψη η ομάδα ανάλυσης παρουσιάζει την στρατηγική προστασίας, τα σχέδια μείωσης των κινδύνων και το σχέδιο δράσης στην γενική διεύθυνση του οργανισμού.

Οι διευθυντές επιθεωρούν και διορθώνουν την στρατηγική και τα σχέδια όπου χρειάζεται και έπειτα αποφασίζουν για τα επόμενα βήματα μετά την ανάλυση κινδύνων. Τα βήματα που ακολουθούνται είναι τα εξής:

-Προετοιμασία για συνάντηση με τους διευθυντές
-Παρουσίαση των πληροφοριών για τους κινδύνους

-Επιθεώρηση και βελτίωση (διόρθωση) της στρατηγικής προστασίας, των σχεδίων μείωσης κινδύνων και του σχεδίου δράση

- Σχεδιασμός επόμενων βημάτων

Αφού ο οργανισμός αναπτύξει στρατηγική προστασίας και σχέδια μείωσης κινδύνων, όλα είναι έτοιμα για την υλοποίηση τους και η μέθοδος OCTAVE τελειώνει[10].

3.2.2 Μέθοδος Security By Analysis (SBA)

Η SBA (Security By Analysis)[11] αναπτύχθηκε στη Σουηδία στις αρχές της δεκαετίας του '80. Αν και είναι ελάχιστα γνωστή εκτός της Σκανδιναβικής χερσονήσου, αποτελεί την πλέον δημοφιλή και ευρέως εφαρμοζόμενη μέθοδο ανάλυσης επικινδυνότητας στη Σουηδία. Η SBA θα πρέπει να θεωρείται λιγότερο ως αυστηρή μέθοδος και περισσότερο ως μία ανθρωποκεντρική οπτική απέναντι στο ζήτημα της ανάλυσης επικινδυνότητας.

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

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

Η SBA Check χρησιμοποιείται για την ταχεία αποτίμηση του επιπέδου ασφάλειας ενός πληροφοριακού συστήματος. Αποτελείται κατά βάση από μία σειρά ερωτηματολογίων, που εστιάζουν, κυρίως, στη διαχείριση της ασφάλειας του συστήματος, έχοντας ως σημείο αναφοράς το πρότυπο ISO/IEC 17799 [9] και ακολουθώντας το κλασικό μοντέλο του καταλόγου (checklist model).

[10,11] *Νικήτας Γ.(2004) "Ανάλυση Κινδύνων Πληροφοριακών Συστημάτων"*

Σύμφωνα με το μοντέλο του καταλόγου η ασφάλεια ενός συστήματος ελέγχεται με βάση έναν κατάλογο από ενδεικνυόμενες ενέργειες και μέτρα προστασίας (checklist), που βρίσκουν εφαρμογή σε ένα μεγάλο εύρος διαφορετικών συστημάτων. Η SBA Check είναι ιδιαίτερα εύκολη στην εφαρμογή της και υποστηρίζεται από ειδικό λογισμικό.

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

- *Main analysis*: Πλήρης ανάλυση με στόχο τον προσδιορισμό της πιθανότητας πραγματοποίησης ενός επεισοδίου ασφάλειας και την εκτίμηση του κόστους με αναλυτικές αριθμητικές μεθόδους.
- *Ten analysis*: Ταχεία ανάλυση με την πιθανότητα και το κόστος να προσδιορίζονται στην κλίμακα 1-10.
- *Risk window*: Συνοπτική ανάλυση βασισμένη σε μία ποιοτική κλίμακα τεσσάρων βαθμίδων.

Η SBA Scenario περιλαμβάνει τα εξής τέσσερα στάδια:

1. Προετοιμασία (Preparation).
2. Σενάρια (Scenarios).
3. Σύνοψη (Overview).
4. Σχέδιο Δράσης (Action Plan).

Στάδιο 1ο

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

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

Στάδιο 2ο

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

Ανάλυση επικινδυνότητας

Αρχικά, το κάθε σενάριο περιγράφεται αναλυτικά και καταγράφονται όλα τα διαθέσιμα στοιχεία που αφορούν το σενάριο, όπως τα γεγονότα που δύναται να οδηγήσουν στην πραγματοποίηση του σεναρίου κ.λπ. Επίσης, εκτιμάται η πιθανότητα το σενάριο να γίνει πραγματικότητα. Ακολούθως οι πιθανές συνέπειες από την πραγματοποίηση του σεναρίου προσδιορίζονται και αναλύονται, ώστε να εκτιμηθεί η σοβαρότητά τους και να προσδιοριστεί ποσοτικά το κόστος που αναμένεται να προκύψει.

Διαχείριση επικινδυνότητας

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

Στάδιο 3^{ο} (σύνοψη)

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

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

Στάδιο 4^{ο} (σχέδιο δράσης)

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

3.2.3 Μέθοδος Marion

Η μέθοδος MARION[12] αναπτύχθηκε στη Γαλλία από τον οργανισμό CLUSIF (Club de la Sécurité des Systèmes d'Information Français) το 1987. Η τελευταία έκδοσή της (1998) περιλαμβάνει τέσσερις φάσεις.

Φάση 0 : Προετοιμασία

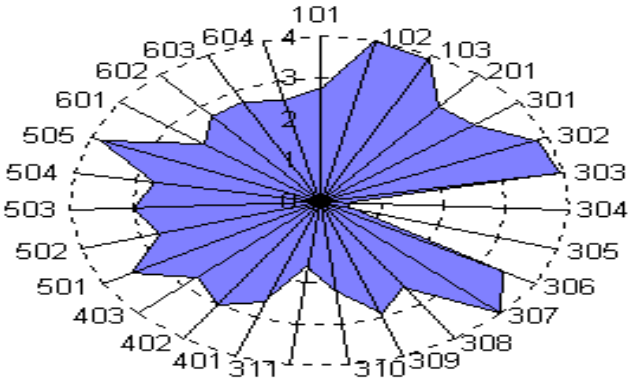
Σε αυτήν τη φάση καθορίζονται οι στόχοι και οροθετείται η ανάλυση. Επίσης, διαμορφώνονται οι ομάδες εργασίας και γίνεται ο προγραμματισμός των εργασιών.

Φάση 1 : Επιθεώρηση των αδυναμιών του συστήματος

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

---

[12]*Κοκολάκης Σπ. "Ανάλυση , αποτίμηση και διαχείριση επικινδυνότητας ΠΣ"*



*(*Σχ.9 Η "ροζέτα" της MARION*)*

Φάση 2: Ανάλυση κινδύνων

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

Φάση 3: Σχέδιο δράσης

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

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

3.2.4 Μέθοδος CRAMM

Η CRAMM (CCTA Risk Analysis and Management Method) αναπτύχθηκε από την Κεντρική Υπηρεσία Υπολογιστών και Τηλεπικοινωνιών (Central Computer and Telecommunications Agency – CCTA) του Ενωμένου Βασιλείου το 1987 [10]. Αποτελεί πρότυπο και εφαρμόζεται από τους οργανισμούς του ευρύτερου δημόσιου τομέα στο Ενωμένο Βασίλειο. Είναι η πιο διαδεδομένη μέθοδος, τουλάχιστον στον ευρωπαϊκό χώρο και έχει εφαρμοστεί με επιτυχία σε μεγάλο αριθμό μεσαίων και μεγάλων οργανισμών.

Η μέθοδος συνοδεύεται και από λογισμικό υποστήριξης, το οποίο βρίσκεται ήδη στην πέμπτη έκδοση. Υποστηρίζει όλα τα βήματα της μεθόδου και αποτελεί αναπόσπαστο τμήμα της. Μέσω του λογισμικού παρακολουθείται η ορθή, βήμα-προς-βήμα, εφαρμογή της μεθοδολογίας, ενώ αποθηκεύονται όλα τα στοιχεία που συλλέγονται κατά την εφαρμογή της. Επίσης, υποστηρίζει όλους τους σύνθετους υπολογισμούς που απαιτούνται για τον προσδιορισμό της επικινδυνότητας, ενσωματώνει μία βιβλιοθήκη

αντιμέτρων και τους μηχανισμούς συμπερασματολογίας που επιλέγουν τα αντίμετρα. Τέλος, παρέχει αναφορές (reports) για όλα τα στάδια της μεθόδου.

Πριν την έναρξη της μελέτης πραγματοποιείται συνάντηση της ομάδας εργασίας με τη Διοίκηση του οργανισμού. Στη συνάντηση αυτή προσδιορίζονται:

- Τα όρια της μελέτης.
- Οι χρήστες των δεδομένων και τα άτομα που θα συνεργαστούν για τη μελέτη.
- Η εξασφάλιση εξουσιοδότησης για άντληση των απαιτούμενων στοιχείων και για διεξαγωγή των συνεντεύξεων.
- Το χρονοδιάγραμμα και το πλάνο διεξαγωγής της μελέτης.

Στη συνέχεια, η ανάλυση και διαχείριση επικινδυνότητας σύμφωνα με την CRAMM ακολουθεί τρία κύρια στάδια):

1. Προσδιορισμός και αξιολόγηση των Αγαθών (identification and valuation of assets).
2. Ανάλυση Επικινδυνότητας (risk analysis).
3. Διαχείριση Επικινδυνότητας (risk management).

Στάδιο	**Βήματα ανά Στάδιο**
Στάδιο 1. Προσδιορισμός και αξιολόγηση των αγαθών *(identif-ication and valuation of assets)*	*Βήμα 1.1*: Δημιουργία του μοντέλου του ΠΣ. *Βήμα 1.2*: Αποτίμηση των στοιχείων-αγαθών του ΠΣ. *Βήμα 1.3*: Επιβεβαίωση και επικύρωση της αποτίμησης.
Στάδιο 2. Ανάλυση Επικινδυνότητας *(risk analysis)*	*Βήμα 2.1*: Προσδιορισμός των Απειλών που αφορούν το κάθε Αγαθό *(asset).* *Βήμα 2.2*: Εκτίμηση Απειλών *(threat assessment)* και Αδυναμιών-Σημείων Ευπάθειας *(vulnerability assessment)* *Βήμα 2.3*: Υπολογισμός Επικινδυνότητας για κάθε συνδυασμό Αγαθού-Απειλής. *Βήμα 2.4*: Επιβεβαίωση και επικύρωση του Βαθμού Επικινδυνότητας.
Στάδιο 3. Διαχείριση Επικινδυνότητας *(risk management)*	*Βήμα 3.1*: Προσδιορισμός της λίστας των προτεινόμενων Αντιμέτρων *(safeguards- countermeasures).* *Βήμα 3.2*: Κατάρτιση Σχεδίου – Πλάνου Ασφάλειας *(security plan).*

(Σχ.10 Στάδια και βήματα εκπόνησης μελέτης Διαχείρισης Επικινδυνότητας)

Στάδιο 1ο: Προσδιορισμός και αξιολόγηση των Αγαθών

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

- **Βήμα 1.1.** Δημιουργία του μοντέλου του ΠΣ.
- **Βήμα 1.2.** Αποτίμηση των στοιχείων του ΠΣ.
- **Βήμα 1.3.** Επιβεβαίωση και επικύρωση της αποτίμησης.

Αναλυτικά, το κάθε επιμέρους βήμα περιλαμβάνει:

Βήμα 1.1: Δημιουργία του μοντέλου του ΠΣ

Αναφέρεται στον προσδιορισμό των στοιχείων του ΠΣ που απαιτούν προστασία. Τα στοιχεία αυτά είναι, κυρίως, τα δεδομένα που χειρίζεται το ΠΣ, όπως επίσης το λογισμικό και το υλικό του ΠΣ. Τα στοιχεία αυτά βρίσκονται σε αλληλεπίδραση. Για παράδειγμα, τα δεδομένα τυγχάνουν επεξεργασίας από το λογισμικό, το οποίο υποστηρίζεται από στοιχεία του υλικού, όπως υπολογιστές, δικτυακός εξοπλισμός και περιφερειακά.

Η προστασία των δεδομένων προϋποθέτει την προστασία του λογισμικού και του υλικού που αποθηκεύει και επεξεργάζεται τα δεδομένα. Επιπλέον, αναγκαία είναι και η προστασία των επικοινωνιακών μέσων που χρησιμοποιούνται για τη μεταφορά των δεδομένων. Για το λόγο αυτό, στα πλαίσια της μεθοδολογίας δημιουργείται ένα μοντέλο του συστήματος, που παρουσιάζει τις συσχετίσεις μεταξύ των στοιχείων του ΠΣ. Η δημιουργία του μοντέλου ακολουθεί τα εξής βήματα:

- Προσδιορισμός των δεδομένων που επεξεργάζεται το ΠΣ και δημιουργία ομάδων δεδομένων.
- Προσδιορισμός των υλικών στοιχείων (physical assets) που υποστηρίζουν την επεξεργασία των δεδομένων.
- Προσδιορισμός των χώρων όπου βρίσκονται τα υλικά στοιχεία.
- Προσδιορισμός του λογισμικού που χρησιμοποιείται στην επεξεργασία των δεδομένων.
- Δημιουργία των μοντέλων που συσχετίζουν τα παραπάνω.

Η συλλογή των παραπάνω στοιχείων βασίζεται στην τεκμηρίωση (documentation) του συστήματος και στον πρώτο κύκλο συνεντεύξεων, που αφορά το τεχνικό προσωπικό και τους κύριους χρήστες του συστήματος.

Αυτές οι δύο κατηγορίες προσωπικού μπορούν να προσφέρουν σημαντικά στοιχεία στην κατεύθυνση της απόκτησης πλήρους εικόνας για τα δεδομένα που χειρίζεται το σύστημα και για τη διάρθρωση του συστήματος. Το μοντέλο του συστήματος εισάγεται στο λογισμικό της CRAMM και ελέγχεται η συνέπειά του (consistency).

Βήμα 1.2: Αποτίμηση των στοιχείων του ΠΣ

Κατά την αποτίμηση των στοιχείων του ΠΣ ιδιαίτερη έμφαση δίδεται στην αποτίμηση των δεδομένων που διαχειρίζεται το ΠΣ. Ο στόχος είναι να προσδιοριστεί η σπουδαιότητα που έχουν τα δεδομένα για τον οργανισμό. Έτσι, μπορούμε να εντοπίσουμε εκείνες τις κατηγορίες δεδομένων που χρήζουν ιδιαίτερης προστασίας και συγκεκριμένα το είδος της προστασίας που απαιτείται.

Η αξία κάθε ομάδας/κατηγορίας δεδομένων αποτιμάται με βάση την επίπτωση (impact) που θα είχε η απώλεια των δεδομένων. Συγκεκριμένα εξετάζεται το μέγεθος της επίπτωσης στις περιπτώσεις της καταστροφής, της μη-εξουσιοδοτημένης μεταβολής (modification), της αποκάλυψης (disclosure) και της μη-διαθεσιμότητας (unavailability). Ειδικότερα, εξετάζονται οι εξής περιπτώσεις:

- *Μη-διαθεσιμότητα* [Λιγότερο από 15 λεπτά, 1 ώρα, 3 ώρες, 12 ώρες, 1 μέρα, 2 μέρες, 1 εβδομάδα, 2 εβδομάδες, 1 μήνα, 2 μήνες και περισσότερο].
- *Καταστροφή* [Απώλεια των δεδομένων μετά την τελευταία λήψη εφεδρικού αντιγράφου. Απώλεια όλων των δεδομένων μαζί με το αντίγραφο].
- *Αποκάλυψη* [Αποκάλυψη των δεδομένων σε άτομα εντός του οργανισμού. Αποκάλυψη των δεδομένων σε άτομα εκτός του οργανισμού. Αποκάλυψη των δεδομένων σε παροχείς υπηρεσιών]
- *Μη-εξουσιοδοτημένη μεταβολή* [Μικρής έκτασης λάθη. Μεγάλης έκτασης λάθη].
- *Ηθελημένη μεταβολή των δεδομένων*.
- *Λάθη μετάδοσης δεδομένων*.

Για κάθε περίπτωση εκτιμάται το χειρότερο πιθανό σενάριο και υπολογίζονται οι επιπτώσεις από την πραγματοποίησή του. Το μέγεθος της επίπτωσης εκτιμάται ποσοτικά με βάση την κλίμακα 1-10. Η μεθοδολογία παρέχει οδηγίες (guidelines) για την αποτίμηση των επιπτώσεων που ανήκουν στις παρακάτω κατηγορίες:

- Επιπτώσεις που αφορούν τη σωματική ακεραιότητα και τη ζωή φυσικών προσώπων.
- Επιπτώσεις από την αποκάλυψη προσωπικών πληροφοριών.
- Νομικές επιπτώσεις.
- Παρεμπόδιση της εφαρμογής της δικαιοσύνης και της εξιχνίασης αξιόποινων πράξεων.
- Οικονομικές απώλειες.
- Διατάραξη της δημόσιας τάξης.
- Εφαρμογή της πολιτικής του οργανισμού.
- Απώλεια της εμπιστοσύνης του κοινού στον οργανισμό.

Επίσης, αποτιμώνται το λογισμικό και το υλικό του ΠΣ. Η αποτίμησή τους γίνεται βάσει του κόστους αντικατάστασής τους. Τέλος, το λογισμικό της CRAMM, βάσει του μοντέλου του ΠΣ, υπολογίζει την έμμεση αξία (implied value) των στοιχείων του ΠΣ. Για παράδειγμα, η απώλεια ενός υπολογιστή (π.χ. κλοπή) συνεπάγεται και απώλεια, έστω προσωρινή, των δεδομένων που επεξεργάζεται και η αξία των τελευταίων θα πρέπει να προστεθεί στην αξία του υπολογιστή.

Η αποτίμηση των στοιχείων του ΠΣ βασίζεται σε συνεντεύξεις που γίνονται με χρήση δομημένων ερωτηματολογίων. Συνεντεύξεις λαμβάνονται τόσο από το τεχνικό, όσο και από το διοικητικό προσωπικό, καθώς και από τους "χρήστες" των υπηρεσιών του συστήματος (π.χ. τους υπαλλήλους που εισάγουν και επεξεργάζονται τα δεδομένα του συστήματος).

Βήμα 1.3: Επιβεβαίωση και επικύρωση της αποτίμησης

Η αποτίμηση των στοιχείων του ΠΣ αποτελεί κρίσιμο παράγοντα για τη διεξαγωγή της Ανάλυσης Επικινδυνότητας. Για αυτόν το λόγο, σε αυτό το σημείο θα πρέπει η αποτίμηση να επιβεβαιωθεί από τη διοίκηση του οργανισμού. Η ομάδα εργασίας παρουσιάζει με τη μορφή έκθεσης τα αποτελέσματα του πρώτου σταδίου στη διοίκηση.

Τα αποτελέσματα εξετάζονται από κοινού κατά τη διάρκεια σύσκεψης και επικυρώνονται. Το κύριο προϊόν αυτού του σταδίου είναι η αποτίμηση των Αγαθών του ΠΣ, η οποία περιλαμβάνει:

- Τον ορισμό του προς ανάλυση συστήματος και των ορίων του.
- Τη μέθοδο εργασίας που ακολουθήθηκε.
- Την αποτίμηση των δεδομένων, του υλικού και του λογισμικού του ΠΣ.
- Γενικά συμπεράσματα του πρώτου σταδίου.

Στάδιο 2^{ο} : Ανάλυση Επικινδυνότητας

Στο πρώτο στάδιο υπολογίστηκε ο ένας από τους τρεις παράγοντες που συνθέτουν την επικινδυνότητα. Συγκεκριμένα, αποτιμήθηκε η αξία των στοιχείων του ΠΣ, τα οποία εφόσον έχουν σημαντική αξία ονομάζονται Αγαθά ή Περιουσιακά Στοιχεία. Στο δεύτερο στάδιο υπολογίζονται οι άλλοι δύο παράγοντες, που είναι το επίπεδο των Απειλών (threat level) και το επίπεδο των Αδυναμιών του συστήματος (vulnerability level). Ο συνδυασμός αυτών των τριών παραγόντων θα μας δώσει το Βαθμό Επικινδυνότητας του συστήματος, έτσι ώστε να επιλεγούν τα κατάλληλα Αντίμετρα. Τα βήματα που ακολουθεί το δεύτερο στάδιο είναι:

- **Βήμα 2.1.**Προσδιορισμός των Απειλών που αφορούν το κάθε Αγαθό.
- **Βήμα 2.2.**Εκτίμηση των Απειλών και Αδυναμιών.
- **Βήμα 2.3.**Υπολογισμός της επικινδυνότητας για κάθε συνδυασμό Αγαθού-Απειλής.
- **Βήμα 2.4.**Επιβεβαίωση και επικύρωση του Βαθμού Επικινδυνότητας.

Αναλυτικά το κάθε επιμέρους βήμα περιλαμβάνει:

Βήμα 2.1: Προσδιορισμός των Απειλών που αφορούν το κάθε Αγαθό (asset)

Η μέθοδος δεν περιορίζεται στον προσδιορισμό των πιθανών Απειλών που καλείται να αντιμετωπίσει ένα ΠΣ γενικά, αλλά επικεντρώνεται στον προσδιορισμό συγκεκριμένων Απειλών για κάθε Αγαθό του ΠΣ.

Η CRAMM παρέχει έναν ενδεικτικό κατάλογο Απειλών, καθώς και συστάσεις για το ποιες κατηγορίες Αγαθών ενός ΠΣ απειλούνται, συνήθως, από τη συγκεκριμένη Απειλή.

Το λογισμικό, έχοντας ένα πλήρες μοντέλο του ΠΣ, έχει τη δυνατότητα να συνυπολογίσει πως όταν ένα από τα Αγαθά του ΠΣ αντιμετωπίζει μία Απειλή, τότε και τα δεδομένα ή οι υπηρεσίες που αυτό υποστηρίζει αντιμετωπίζουν την ίδια Απειλή. Για παράδειγμα, όταν ένας υπολογιστής αντιμετωπίζει την Απειλή της κλοπής, τότε και τα δεδομένα που αυτός έχει αποθηκευμένα κινδυνεύουν να κλαπούν μαζί του. Έτσι ο αναλυτής δεν χρειάζεται να υπολογίζει ο ίδιος όλες τις συσχετίσεις και αλληλεπιδράσεις.

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

Βήμα 2.2: Εκτίμηση Απειλών (threat assessment) και Αδυναμιών (vulnerability assessment)

Για κάθε συνδυασμό Απειλής-Αγαθού γίνεται εκτίμηση του μεγέθους της Απειλής και της σοβαρότητας των Αδυναμιών που μπορεί να οδηγήσουν στην πραγματοποίηση της Απειλής. Η εκτίμηση αυτή γίνεται βάσει δομημένων ερωτηματολογίων. Η εκτίμηση της Απειλής γίνεται στην κλίμακα 1-5 (very low, low, medium, high, very high), αυτόματα από το εργαλείο, βάσει των απαντήσεων που δόθηκαν στα ερωτηματολόγια. Αντίστοιχα για τις Αδυναμίες συμπληρώνονται τα ερωτηματολόγια των Αδυναμιών και υπολογίζεται η σοβαρότητα της Αδυναμίας στην κλίμακα 1-3 (low, medium, high). Οι απαντήσεις που θα δοθούν στα ερωτηματολόγια προκύπτουν από τα στοιχεία που συλλέγουν οι αναλυτές από τους χρήστες του συστήματος.

Το εργαλείο παρέχει ερωτηματολόγια για κάθε συνδυασμό Απειλής - Αγαθού. Οι απαντήσεις των ερωτηματολογίων εισάγονται στο εργαλείο και εκείνο υπολογίζει το επίπεδο των Απειλών και των Αδυναμιών. Επίσης, παρέχει τη δυνατότητα στους αναλυτές να αλλάξουν τις τιμές που υπολογίστηκαν αυτόματα. Τέλος, μας παρέχει μία αναφορά για την εκτίμηση των Απειλών-Αδυναμιών, ώστε να αξιολογηθούν τα αποτελέσματα αυτής της διαδικασίας.

Βήμα 2.3: Υπολογισμός επικινδυνότητας για κάθε συνδυασμό Αγαθού-Απειλής

Η CRAMM υπολογίζει το Βαθμό Επικινδυνότητας για κάθε συνδυασμό Αγαθού-Απειλής. Δεν έχουμε, δηλαδή, απλώς ένα Βαθμό Επικινδυνότητας για το ΠΣ στο σύνολό του, αλλά έχουμε συγκεκριμένη αποτίμηση της επικινδυνότητας για κάθε επιμέρους συνδυασμό Αγαθού-Απειλής. Για το σκοπό αυτό, χρησιμοποιούνται τόσο τα αποτελέσματα της εκτίμησης των Απειλών και των Αδυναμιών, όσο και το μοντέλο του συστήματος που έχει δημιουργηθεί από το πρώτο στάδιο. Έτσι, ο Βαθμός Επικινδυνότητας λαμβάνει υπόψη και τη συσχέτιση μεταξύ των Αγαθών του ΠΣ. Ουσιαστικά ο Βαθμός Επικινδυνότητας απεικονίζει τις απαιτήσεις ασφάλειας για κάθε Αγαθό του ΠΣ, καθώς μεγαλύτερη επικινδυνότητα συνεπάγεται και υψηλότερη απαίτηση για ασφάλεια. Ο υπολογισμός του Βαθμού Επικινδυνότητας ακολουθεί την κλίμακα 1-7.

Ο Βαθμός Επικινδυνότητας για κάθε συνδυασμό Αγαθού-Απειλής υπολογίζεται από το εργαλείο. Ο αναλυτής έχει τη δυνατότητα να παρέμβει και να αλλάξει κάποιες τιμές, αν το θεωρεί σκόπιμο. Το πλήθος των συνδυασμών Αγαθού-Απειλής και κυρίως η πολυπλοκότητα της αλληλοσυσχέτισης των Αγαθών στα πλαίσια ενός ΠΣ, κάνουν πρακτικά αδύνατο τον εμπειρικό και χειρογραφικό υπολογισμό της επικινδυνότητας.

Βήμα 2.4: Επιβεβαίωση και επικύρωση του Βαθμού Επικινδυνότητας

Ο Βαθμός Επικινδυνότητας θα χρησιμοποιηθεί στο επόμενο στάδιο για την επιλογή των Αντιμέτρων. Συνεπώς, η ορθότητα των εκτιμήσεων που έγιναν κατά τη διάρκεια του δεύτερου σταδίου θα πρέπει να ελεγχθεί πριν προχωρήσουμε στο επόμενο στάδιο της μεθοδολογίας. Σε περίπτωση που κριθεί ότι χρειάζεται να γίνουν κάποιες αλλαγές, τότε οι αναλυτές έχουν τη δυνατότητα είτε να αλλάξουν απευθείας τις τιμές της επικινδυνότητας, είτε να αλλάξουν τις τιμές που έχουν προκύψει από την εκτίμηση των Απειλών και Αδυναμιών και να υπολογίσουν εκ νέου την επικινδυνότητα.

Σε οποιαδήποτε περίπτωση, τα αποτελέσματα του δεύτερου σταδίου θα πρέπει να εγκριθούν από τη διοίκηση του οργανισμού πριν προχωρήσουμε στο τρίτο στάδιο. Για το σκοπό αυτόν, η ομάδα μελέτης παρουσιάζει με τη μορφή έκθεσης τα αποτελέσματα του δεύτερου σταδίου στη διοίκηση. Τα αποτελέσματα εξετάζονται από κοινού με τη διοίκηση, κατά τη διάρκεια σύσκεψης, και επικυρώνονται από αυτήν.
Το κύριο προϊόν αυτού του σταδίου είναι η Αποτίμηση της Επικινδυνότητας, η οποία περιλαμβάνει:

- Περιγραφή των Απειλών και των Αδυναμιών που συνδέονται με αυτές.
- Την εκτίμηση της σοβαρότητας κάθε Απειλής και Αδυναμίας.
- Την εκτίμηση του Βαθμού Επικινδυνότητας για κάθε συνδυασμό Αγαθού-Απειλής.
- Γενικά συμπεράσματα σχετικά με την επικινδυνότητα του ΠΣ.

Στάδιο 3^{ο} : Διαχείριση Επικινδυνότητας

Με βάση τα αποτελέσματα της Ανάλυσης Επικινδυνότητας (2ο στάδιο), η CRAMM παράγει ένα προτεινόμενο Σχέδιο Ασφάλειας (security plan). Αυτό αποτελείται από μία σειρά Αντιμέτρων, τα οποία θεωρούνται απαραίτητα για τη Διαχείριση της Επικινδυνότητας και τα οποία θα πρέπει να εφαρμοστούν στο ΠΣ. Το Σχέδιο Ασφάλειας περιλαμβάνει και μία σειρά εναλλακτικών επιλογών, ώστε να παρέχεται ευελιξία στην εφαρμογή του.

Για συστήματα τα οποία έχουν αναπτυχθεί και λειτουργούν ήδη, το προτεινόμενο Σχέδιο Ασφάλειας μπορεί να συσχετισθεί με τα υπάρχοντα Αντίμετρα. Η τελική επιλογή των Αντιμέτρων που θα εφαρμοστούν λαμβάνει υπόψη και το κόστος που έχουν τα Αντίμετρα για τον οργανισμό. Τα βήματα του τρίτου σταδίου περιλαμβάνουν:

- **Βήμα 3.1.** Προσδιορισμός της λίστας των προτεινόμενων Αντιμέτρων.
- **Βήμα 3.2.** Κατάρτιση του Σχεδίου Ασφάλειας.

Αναλυτικά το κάθε επιμέρους βήμα περιλαμβάνει:

Βήμα 3.1: Προσδιορισμός της λίστας των προτεινόμενων Αντιμέτρων

Το λογισμικό της CRAMM διαθέτει μία βάση Αντιμέτρων. Τα Αντίμετρα αυτά είναι τεχνικά, διοικητικά και οργανωτικά. Το λογισμικό επιλέγει αυτόματα έναν κατάλογο προτεινόμενων Αντιμέτρων, με βάση τα αποτελέσματα της Ανάλυσης Επικινδυνότητας. Τα Αντίμετρα αυτά χωρίζονται σε ομάδες ανάλογα με το είδος των Απειλών που καλούνται να αντιμετωπίσουν και το είδος των Αγαθών που καλούνται να προστατέψουν. Η κατάσταση των Αντιμέτρων περιλαμβάνει τις εναλλακτικές λύσεις, δηλαδή ποιο Αντίμετρο μπορεί να χρησιμοποιηθεί στη θέση ενός άλλου.

Από τον προτεινόμενο κατάλογο θα πρέπει να γίνουν συγκεκριμένες επιλογές. Οι επιλογές αυτές βασίζονται σε μεγάλο βαθμό στην εμπειρία των αναλυτών. Η CRAMM, όμως, βοηθά ώστε οι επιλογές αυτές να ακολουθούν μία δομημένη προσέγγιση και να αιτιολογούνται επαρκώς. Τα κριτήρια που λαμβάνονται υπόψη στην τελική επιλογή περιλαμβάνουν μεταξύ άλλων και τα εξής:

- Την επίδραση που θα έχουν τα Αντίμετρα στη λειτουργία του οργανισμού.
- Τον υπάρχοντα προϋπολογισμό (budget) για την ασφάλεια του ΠΣ.
- Το κόστος εγκατάστασης και λειτουργίας των Αντιμέτρων, τόσο όσον αφορά το χρηματικό κόστος, όσο και το κόστος σε ανθρώπινους πόρους.
- Τα μελλοντικά σχέδια του οργανισμού για ανάπτυξη ή επέκταση του συστήματος.
- Την άποψη της διοίκησης και τους στόχους της.
- Τις ενδείξεις ότι οι Απειλές θα αυξηθούν στο μέλλον.
- Την αποτελεσματικότητα των Αντιμέτρων.

Αναφορικά με το τελευταίο κριτήριο, τα Αντίμετρα χωρίζονται στις εξής κατηγορίες, ανάλογα με το στόχο τους:

- Μείωση των Απειλών.
- Μείωση των Αδυναμιών.
- Μείωση της Επίπτωσης.

- Ανίχνευση της παραβίασης της ασφάλειας.
- Ανάκαμψη (recovery).

Η παραπάνω κατηγοριοποίηση παρουσιάζει τα Αντίμετρα κατά φθίνουσα σειρά αποτελεσματικότητας. Τέλος, τα προτεινόμενα Αντίμετρα συγκρίνονται με τα υπάρχοντα. Είναι συχνά προτιμότερο να παραμείνει ένα από τα υπάρχοντα Αντίμετρα, παρά να αντικατασταθεί από κάποιο ισοδύναμό του. Η βιβλιοθήκη Αντιμέτρων περιλαμβάνει περίπου 2.000 αντίμετρα, χωρισμένα σε ομάδες και ιεραρχημένα ανάλογα με το επίπεδο ασφάλειας που προσφέρουν. Το λογισμικό επιλέγει αυτόματα τα Αντίμετρα σύμφωνα με τα αποτελέσματα της Ανάλυσης Επικινδυνότητας. Δίνει τη δυνατότητα να παρακολουθήσουμε την εφαρμογή τους μέσω της λειτουργίας *"Κατάσταση Υλοποίησης Αντιμέτρων" (Maintain Countermeasure Implementation State)*. Ένα Αντίμετρο μπορεί να βρίσκεται σε μία από τις ακόλουθες καταστάσεις:

- Εγκατεστημένο (*installed*).
- Επιλεγμένο για εγκατάσταση (*to be installed*).
- Υπό υλοποίηση (*implementing recommendation*).
- Έχει υλοποιηθεί (*implemented recommendation*).
- Έχει ήδη καλυφθεί από άλλο αντίμετρο (*already covered*).
- Αναλαμβάνεται η επικινδυνότητα και δεν υλοποιείται (*accept level of risk*).
- Υπό συζήτηση (*under discussion*).
- Μη εφαρμόσιμο (*not applicable*).

Βήμα 3.2: Κατάρτιση Σχεδίου - Πλάνου Ασφάλειας

Στο τελευταίο βήμα καταρτίζεται το Σχέδιο Ασφάλειας, το οποίο περιλαμβάνει:

- Την Πολιτική Ασφάλειας.
- Το σχέδιο Εφαρμογής των Αντιμέτρων.

Η CRAMM παρέχει μία δομή Πολιτικής Ασφάλειας. Για τη δημιουργία της Πολιτικής Ασφάλειας μπορεί να χρησιμοποιηθούν οι οδηγίες πολιτικής (policy statements) που παράγονται μαζί με τη λίστα των Αντιμέτρων. Μια πρώτη ενέργεια που γίνεται συνήθως είναι να προσδιοριστούν οι ρόλοι (π.χ. υπεύθυνος ασφάλειας, διαχειριστής συστήματος κ.λπ.) και να περιγραφούν οι αρμοδιότητες του καθ' ενός.

Το Σχέδιο Εφαρμογής των Αντιμέτρων περιέχει τις περαιτέρω ενέργειες, που πρέπει να γίνουν για την ασφάλεια του ΠΣ. Κεντρικό του στοιχείο είναι το σύνολο των Αντιμέτρων, τα οποία όμως ιεραρχούνται με βάση τις προτεραιότητες εφαρμογής τους. Το Σχέδιο Ασφάλειας αποτελεί το κύριο προϊόν του τρίτου σταδίου και όλου του έργου[13].

---

[13]*ΚΟΚΟΛΑΚΗΣ ΣΠ. "Ανάλυση , αποτίμηση και διαχείριση επικινδυνότητας ΠΣ"*

3.2.5 Λογισμικό ανάλυσης κινδύνου

Εισαγωγή

Η ανάλυση κινδύνων δεν είναι απλή διαδικασία και συνήθως παράγει ένα πολύ μεγάλο αριθμό δεδομένων για επεξεργασία. Όσο μεγαλύτερο δε το εύρος της ανάλυσης, τόσο πιο δύσκολη είναι η διαχείριση των πληροφοριών που συλλέγονται. Αναγνωρίζοντας την παραπάνω δυσκολία, πολλές εταιρίες έχουν αναπτύξει λογισμικό για την διευκόλυνση της ανάλυσης κινδύνων. Στις περισσότερες περιπτώσεις οι εταιρίες έχουν αναπτύξει τις δικές τους παραλλαγές μεθόδων ανάλυσης κινδύνων που υποβοηθούνται από το λογισμικό. Η εξέλιξη αυτή βοήθησε σημαντικά την απλοποίηση της ανάλυσης κινδύνων ώστε να μπορεί πλέον να γίνεται στο εσωτερικό ενός οργανισμού με ελάχιστη ή καθόλου παρέμβαση από εξωτερικούς ειδικούς. Τα πακέτα λογισμικού ανάλυσης κινδύνων που κυκλοφορούν στην αγορά είναι πλέον αρκετά και καλύπτουν διαφορετικές ανάγκες και απαιτήσεις. Στο κεφάλαιο αυτό περιγράφονται τα βασικά χαρακτηριστικά και δυνατότητες που προσφέρουν τα σύγχρονα πακέτα λογισμικού ανάλυσης κινδύνων και γίνεται μια προσπάθεια παρουσίασης μερικών από αυτών που βρέθηκαν ύστερα από σύντομη αναζήτηση στο Internet (με αλφαβητική σειρά).

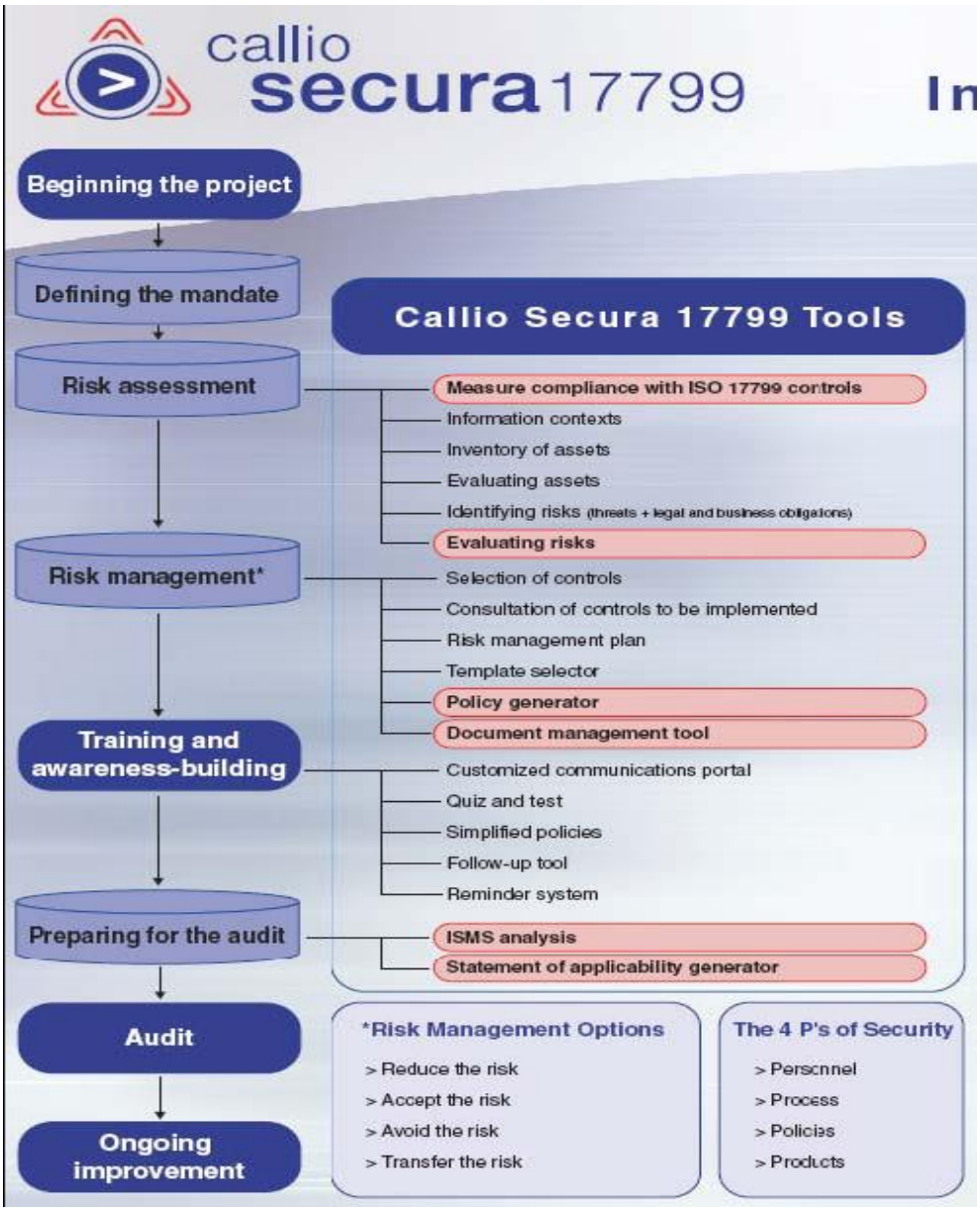
Callio Secura 17799

Το Callio Secura 17799 είναι προϊόν μιας σχετικά καινούργιας εταιρίας που ειδικεύεται στην ασφάλεια πληροφοριακών συστημάτων, της Callio Technologies που ιδρύθηκε το 2001 στον Καναδά. Το Callio Secura 17799 είναι ένα σύστημα διαχείρισης ασφάλειας πληροφοριακών συστημάτων με έμφαση την συμμόρφωση με το διεθνές στάνταρ BS7799 / ISO 17799.Βασίζεται σε μια δική του μέθοδο για την ανάλυση κινδύνων που είναι σχετικά απλή, βήμα προς βήμα, ώστε να γίνεται εύκολα κατανοητή και να μην απαιτεί ειδικευμένο προσωπικό για την χρήση του. Ανήκει δε στην κατηγορία των ποιοτικών μεθόδων. Περιλαμβάνει ολοκληρωμένα εργαλεία για:

- την αποτίμηση των κινδύνων,
- την αντιμετώπιση τους,
- την δημιουργία πολιτικών ασφαλείας,
- την διαχείριση εγγράφων,
- την δημιουργία αναφορών, και τέλος αυτό που την κάνει να ξεχωρίζει,
- την εκπαίδευση του προσωπικού.

Μια άλλη βασική του διαφορά σε σχέση με τον ανταγωνισμό είναι ότι τρέχει σε αρχιτεκτονική http(ColdFusion) σε ένα server, και η διαχείριση του προγράμματος γίνεται από οποιοδήποτε υπολογιστή (και λειτουργικό σύστημα) μέσω ενός απλού web browser. Το πρόγραμμα δημιουργεί ένα web site στο οποίο μπορούν να έχουν πρόσβαση από παντού όσοι συμμετέχουν στην ανάλυση κινδύνων και χρησιμοποιείται επίσης για την ενημέρωση και εκπαίδευση του προσωπικού για τα θέματα ασφαλείας, τις υπάρχουσες πολιτικές ασφαλείας, τις διαδικασίες κτλ. Το πρόγραμμα διατηρεί βάση δεδομένων στον server με πλήρης δυνατότητα δικαιωμάτων και ομάδων χρηστών έτσι ώστε ο κάθε χρήστης να βλέπει ή να αλλάζει μόνο τα αρχεία εκείνα που τον αφορούν. Περιέχει επίσης όλα εκείνα τα εργαλεία που χρειάζονται για την συνεχή διαχείριση και βελτίωση όλων των εγγράφων ασφαλείας του οργανισμού (πχ. version control). Το interface του προγράμματος είναι πολύ εύκολο και χρηστικό και δεν χρειάζεται ειδική εκπαίδευση για την χρησιμοποίηση του. Παρακάτω δίνεται ένα διάγραμμα που δείχνει τα εργαλεία που προσφέρει το Callio Secura 17799 για κάθε βήμα της ανάλυσης κινδύνων[14].

[14] *ΝΙΚΗΤΑΣ Γ..(2004) "Ανάλυση Κινδύνων Πληροφοριακών Συστημάτων"*



(Σχ.11 Απόκομμα από το φυλλάδιο του Callio Secura 17799)

COBRA

Το πρόγραμμα COBRA[15] είναι ένα από τα πιο παλιά που κυκλοφορούν στην αγορά. Σχεδιάστηκε από την εταιρία C&A Systems Security Ltd και έχει φτάσει σήμερα στην έκδοση 3. Το πρόγραμμα χρησιμοποιεί την δική του μέθοδο για ανάλυση κινδύνων, η οποία βοηθάει στην επίτευξη συμμόρφωσης με το διεθνές στάνταρ ISO17799/BS7799.

Ένα από τα σημαντικότερα πλεονεκτήματα του είναι η αυτόματη προσαρμογή της ανάλυσης στις συγκεκριμένες ανάγκες του κάθε οργανισμού. Επίσης, για πιο απαιτητικές αναλύσεις επιτρέπεται η πλήρη παραμετροποίηση των γνωσιακών βάσεων που περιέχει (knowledge bases). Περιλαμβάνεται επιπλέον και η λεγόμενη «What if» ανάλυση, κατά την οποία ελέγχονται υποθετικά σενάρια ώστε να διαπιστωθεί δυναμικά η επίδραση που θα έχουν συγκεκριμένα αντίμετρα στους βαθμούς κινδύνου. Τέλος, το πρόγραμμα έχει την δυνατότητα δημιουργίας αναφορών επαγγελματικού επιπέδου που δεν μοιάζουν με τυπικές αναφορές που παράγονται από υπολογιστή. Μάλιστα υπάρχει η δυνατότητα αναφορών που αναφέρονται είτε σε τεχνικό προσωπικό (άρα με γνώσεις σε τεχνικούς όρους) είτε στην διοίκηση του οργανισμού. Το πρόγραμμα τρέχει σε πλατφόρμα MS Windows με ελάχιστες απαιτήσεις αλλά και με interface που παραπέμπει σε λίγο παλαιότερες εποχές.

---

[15] *ΝΙΚΗΤΑΣ Γ..(2004) "Ανάλυση Κινδύνων Πληροφοριακών Συστημάτων"*

ΚΕΦΑΛΑΙΟ 4

ΜΟΝΤΕΛΑ ΔΙΑΧΕΙΡΙΣΗΣ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ

4.1 Το Αντικειμενοστραφές Μοντέλο

Το αντικειμενοστραφές μοντέλο διαχείρισης επικινδυνότητας, προτάθηκε από τον Wahlgren το 1995 . Ορισμένα χαρακτηριστικά της αντικειμενοστραφούς προσέγγισης είναι:

- Υπάρχει δυνατότητα να κληρονομούνται χαρακτηριστικά από γενικότερα αντικείμενα (general objects), γεγονός που διευκολύνει την αποθήκευση πληροφοριών.
- Μπορούν αντικείμενα (object) να επηρεάζουν άλλα αντικείμενα με τη βοήθεια σχέσεων (relations).
- Κατασκευή μοντέλων πολύπλοκων υπολογιστικών συστημάτων.
- Δυνατότητα προσαρμογής του μοντέλου σε περίπτωση προσθήκης ή διαγραφής τμημάτων.
- Δυνατότητα τροποποίησης των χαρακτηριστικών ενός αντικειμένου.

Το αντικειμενοστραφές μοντέλο αποτελείται από αντικείμενα, από τα οποία τα βασικότερα είναι: αγαθά, απειλές, αδυναμίες, μέτρα προστασίας και επικινδυνότητα Υπάρχουν τρία είδη μοντέλων, που περιέχονται και κρίνονται απαραίτητα:

- **Μοντέλο αντικειμένων (Object model):** περιγράφει τη στατική δομή των αντικειμένων -objects- του συστήματος και τις σχέσεις -relations- μεταξύ τους.
- **Δυναμικό μοντέλο (Dynamic model):** περιγράφει τις αλλαγές που συμβαίνουν στο σύστημα με το πέρασμα του χρόνου (γεγονότα -events- και καταστάσεις -states).
- **Μοντέλο λειτουργιών (Functional model):** περιγράφει τους μετασχηματισμούς που υφίστανται τα δεδομένα μέσα στο σύστημα (τιμές -values- και συναρτήσεις -functions).

Αφού κατασκευαστούν τα τρία αυτά μοντέλα, συνδυάζονται με τις καθορισμένες περιγραφές των αντικειμένων (περιέχουν πληροφορίες από το δυναμικό και το μοντέλο λειτουργιών).

[16] *WAHLGREN G. (1995) ‘‘An object oriented approach to an IT risk management system’’, In Information Security - the Next Decade (eds. Ellof J. and S. von Solms), pp.79-86. Proceedings of the 11th International Conference in Information Security, IFIP’ 95, Chapman-Hall, London.*

4.2 Το μοντέλο TOPM (Target Optimum Portfolio Management)

Το μοντέλο TOPM (Target Optimum Portfolio Management) προτάθηκε από το 1994 από τους K. Badenhorst και J. Eloff και αφορά στη διαχείριση της επικινδυνότητας που υπάρχει σε ένα υπολογιστικό σύστημα (information technology). Στις κλασικές μεθοδολογίες ανάλυσης, εκτίμησης και διαχείρισης επικινδυνότητας ορίζονται αυστηρά τις περιοχές του ενδιαφέροντος (π.χ. υλικό, λογισμικό, περιβάλλον, προσωπικό), ενώ το μοντέλο TOPM ακολουθεί διαφορετική προσέγγιση, περισσότερο συνθετική. Στηρίζεται στην έννοια του δυναμικού κύκλου ζωής και έχει στοχεύει στη βελτιστοποίηση της διαδικασίας διαχείρισης επικινδυνότητας. Βασίζεται στον κύκλο ζωής που έχει υιοθετηθεί από τη μεθοδολογία RS (των ιδίων των K. Badenhorst και J. Eloff) μία πλήρη μεθοδολογία για την ανάλυση και υλοποίηση της ασφάλειας μέσα σε ένα οργανισμό.

[17] *ELOFF J.H.P., BADENHORST K.P. (1994) ''TOPM: o formal approach to the optimisation of information technology risk management'', Computers & Security, Vol.13, No.5, pp.411-435.*

ΚΕΦΑΛΑΙΟ 5

ΣΥΓΚΡΙΣΗ ΜΕΘΟΔΟΛΟΓΙΩΝ

5.1 Πλεονεκτήματα – Μειονεκτήματα

Η SBA διακρίνεται για τον ανθρωποκεντρικό και συμμετοχικό της χαρακτήρα. Δίνει ιδιαίτερη βαρύτητα στη συμμετοχή των ανθρώπων που η εργασία τους σχετίζεται με το πληροφοριακό σύστημα και ενθαρρύνει τη δημιουργικότητα και τη φαντασία τους. Τα βασικότερα πλεονεκτήματα της μεθόδου είναι τα εξής:

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

Τα κυριότερα μειονεκτήματα της μεθόδου είναι τα εξής:

- Στηρίζεται σε μεγάλο βαθμό στις ικανότητες, τη φαντασία και τη διάθεση για συνεισφορά των εργαζομένων.
- Προϋποθέτει την ανάπτυξη ανθρωποκεντρικής και συμμετοχικής κουλτούρας. Αυτός είναι, ίσως, ο κυριότερος λόγος που η εφαρμογή της μεθόδου δεν έχει επεκταθεί ιδιαίτερα εκτός των Σκανδιναβικών χωρών.
- Δεν συνοδεύεται από βιβλιοθήκες μέτρων προστασίας. Η επινόηση και ο σχεδιασμός των μέτρων προστασίας επαφίεται στις ομάδες εργασίας.

Για την MARION μπορούμε να παρατηρήσουμε ότι:

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

Η CRAMM, ως μέθοδος ανάλυσης και διαχείρισης επικινδυνότητας, έχει σημαντικά πλεονεκτήματα, τα οποία πηγάζουν κυρίως από το δομημένο και συστηματικό χαρακτήρα της. Τα κυριότερα πλεονεκτήματά της είναι:

- Καλύπτει το σύνολο των σταδίων ανάλυσης και διαχείρισης επικινδυνότητας.
- Καλύπτει όλες τις συνιστώσες της ασφάλειας (π.χ. θέματα προσωπικού, διαδικασιών, τεχνικά θέματα, φυσική ασφάλεια κ.ά.)
- Έχει δοκιμαστεί με επιτυχία και υπάρχει μεγάλη διεθνή εμπειρία από την εφαρμογή της.
- Συνοδεύεται από αυτοματοποιημένο εργαλείο που διευκολύνει την εφαρμογή της και επιλέγει τα αντίμετρα από μία μεγάλη βιβλιοθήκη αντιμέτρων.

Παράλληλα, όμως, παρουσιάζει και ορισμένα μειονεκτήματα, τα κυριότερα από τα οποία είναι:

- Στηρίζεται σε μεγάλο βαθμό στη συνεργασία των αναλυτών με τους χρήστες και τη διοίκηση του οργανισμού και στηρίζεται σημαντικά στις απόψεις των χρηστών.
- Έχει υψηλό κόστος εφαρμογής, από άποψης χρόνου και ανθρώπινης προσπάθειας.
- Στηρίζεται σε ένα πολύ απλοϊκό μοντέλο του πληροφοριακού συστήματος.

- Εστιάζει ουσιαστικά μόνο στα δεδομένα και λαμβάνει υπόψη τον ανθρώπινο παράγοντα μόνο ως απειλή.
- Απαιτεί μερικές φορές την επέμβαση του αναλυτή για την προσαρμογή των αποτελεσμάτων των αυτόματων υπολογισμών.
- Το τελικό αποτέλεσμα στηρίζεται σε μεγάλο βαθμό σε υποκειμενικές εκτιμήσεις, η οποίες όμως συχνά δεν γίνονται αντιληπτές ως τέτοιες.
- Απαιτεί επεξεργασία των προτεινόμενων αντιμέτρων (ομαδοποίηση, εξειδίκευση, κ.λπ.) για την προσαρμογή τους στο υπό μελέτη ΠΣ. Πολλά από τα αντίμετρα είναι πολύ γενικά.

5.2 Επιλογή κατάλληλης μεθόδου

Η επιλογή μίας μεθόδου εξαρτάται από τα ιδιαίτερα χαρακτηριστικά του ΠΣ, στο οποίο πρόκειται να εφαρμοστεί, καθώς και από οικονομικούς και οργανωτικούς παράγοντες. Παρακάτω αναφέρουμε ενδεικτικά ορισμένα από τα κριτήρια επιλογής μίας μεθόδου ανάλυσης και διαχείρισης επικινδυνότητας .

- Να ανταποκρίνεται στο μέγεθος και τη συμπλοκότητα του ΠΣ.
- Να έχει χαμηλό κόστος εφαρμογής.
- Να ταιριάζει στα οργανωσιακά χαρακτηριστικά και τη κουλτούρα του οργανισμού.
- Να υποστηρίζεται από εξειδικευμένο λογισμικό.
- Τα πρόσωπα, που θα κληθούν να την εφαρμόσουν, να έχουν εμπειρία από την εφαρμογή της ή τουλάχιστον να έχουν εκπαιδευτεί σε αυτήν.
- Να καλύπτει όλους τους παράγοντες που συνδέονται με την ασφάλεια των πληροφοριακών συστημάτων (τεχνικούς και κοινωνικούς).

[18] *ΚΟΚΟΛΑΚΗΣ ΣΠ. "Ανάλυση , αποτίμηση και διαχείριση επικινδυνότητας ΠΣ"*

ΚΕΦΑΛΑΙΟ 6

ΣΥΜΠΕΡΑΣΜΑΤΑ

Έχοντας αναλύσει διεξοδικά όλα εκείνα τα χαρακτηριστικά που συνθέτουν την έννοια της ανάλυσης και διαχείρισης επικινδυνότητας και αφού έγινε σύγκριση των μεθοδολογιών που χρησιμοποιούνται ευρέως καταλήγουμε στα παρακάτω συμπεράσματα.

Πρωτίστως, η ανάγκη για ασφάλεια στα πληροφοριακά συστήματα είναι επιτακτική. Κύριος στόχος ενός συστήματος είναι η διατήρηση της ασφάλειάς του. Συνεπώς, η συστηματική μείωση του κινδύνου κ η αντιμετώπιση των απωλειών που μπορεί να προκύψουν σε ένα ΠΣ αφορά στο ερώτημα της επιλογής αντιμέτρων που θα προσφέρουν προστασία ανάλογη των κινδύνων που απειλούν το πληροφοριακό σύστημα κ αυτό ακριβώς είναι η ανάλυση και διαχείριση επικινδυνότητας.

Η ανάλυση και διαχείριση επικινδυνότητας

1. δίνει την δυνατότητα αιτιολόγησης του κόστους των αντιμέτρων
2. είναι εργαλείο επικοινωνίας ανάμεσα στην διοίκηση του οργανισμού και τους ειδικούς των ΠΣ
3. εφαρμόζεται είτε αυτούσια είτε σε συνδυασμό με άλλες μεθόδους
4. δίνει την δυνατότητα για άμεση κατανόηση της λειτουργίας του ΠΣ

και το σημαντικότερο

5. είναι η πιο διαδεδομένη μεθοδολογία σχεδιασμού και διαχείρισης της ασφάλειας ΠΣ.

Έχοντας υπόψιν τις εξής μεθοδολογίες :

1. OCTAVE

Όπως προείπαμε είναι μια αυτό-διευθυνόμενη μέθοδος για ανάλυση κινδύνων, η οποία στηρίζεται στο προσωπικό του οργανισμού, και θα λειτουργήσει ιεραρχικά, για την

ανάλυση και την στρατηγική που θα εφαρμοστεί. Χρειάζεται 3 φάσεις για την ολοκλήρωσή της:

i. **Organizational view** (ανάλυση προβλήματος και ενημέρωση για το πρόβλημα σε Γενική διεύθυνση, Διευθυντές τμημάτων και Προσωπικό)
ii. **Technological view** (Αναγνώριση των κρισιμότερων κατηγοριών συστημάτων και αναγνώριση των συγκεκριμένων συστημάτων που θα εξεταστούν)
iii. **Strategy and plan development** (στρατηγικές ασφαλείας και σχέδια αντιμετώπισης των κινδύνων του οργανισμού)

2. SBA

Μέθοδος βασισμένη στο προσωπικό, ανεξάρτητα από τον ρόλο και την θέση τους, είναι αυτοί που είναι πιθανότερο να εντοπίσουν προβλήματα ασφαλείας λόγω του ότι συμμετέχουν στην καθημερινή λειτουργία του συστήματος.

Οι κυριότερες από τις μεθόδους της είναι οι:

- **SBA Check** (αποτίμηση επιπέδου ασφάλειας ΠΣ)
- **SBA Scenario** (ποσοτική ανάλυση επικινδυνότητας ΠΣ)

Ακολουθείται η εξής διαδικασία:

-Προετοιμασία (Διδάσκεται η SBA από τον ειδικό ασφαλείας στο προσωπικό το οποίο χωρίζεται σε ομάδες για την υλοποίηση)

-Σενάρια (Εντοπισμός και καταγραφή πιθανών σεναρίων προβλήματος ασφάλειας και τι "ζημιά" κόστους προκύπτει σε περίπτωση που πραγματοποιηθούν)

-Σύνοψη (Προσδιορισμός προτεραιοτήτων μέτρων προστασίας, που θα υλοποιηθούν, βάσει ενδεχόμενου κόστους που μπορεί να προκύψει και μείωση επικινδυνότητας μετά την υλοποίηση του μέτρου προστασίας)

-Σχέδιο Δράσης (Καθορισμός υπευθύνων για την υλοποίηση μέτρων προστασίας)

3. MARION

i. **Φάση 0** : Στόχοι, οριοθέτηση ανάλυσης και διαμόρφωση ομάδων εργασιών
ii. **Φάση 1 :** Εντοπισμός και αξιολόγηση σημείων αδυναμίας συστήματος με βοήθεια ερωτηματολογίου και έτσι δημιουργείται ροζέτα με δείκτες ευπάθειας και βαθμό ευπάθειας για κάθε ένα δείκτη ξεχωριστά που έτσι εντοπίζονται οι τομείς που απαιτούν περισσότερη προσοχή
iii. **Φάση 2 :** επεξεργασία δεδομένων από τις προηγούμενες φάσεις και κατηγοριοποίηση κίνδυνων σε μείζονες και απλούς, το ΠΣ χωρίζεται και αναλύεται σε διαφόρους τομείς, βάσει τύπων απειλών
iv. **Φάση 3 :** Επιλογή μέτρων προστασίας με βάσει αποτελεσματικότητα και κόστος

4. CRAMM

Ίσως η πιο ολοκληρωμένη μέθοδος αρκετά διαδεδομένη και με λογισμικό υποστήριξης όλων των βημάτων της.

Μετά από συνάντηση της ομάδας εργασίας με την Διοίκηση του οργανισμού γίνεται προσδιορισμός:

- Ορίου της μελέτης
- Των χρηστών δεδομένων και συνεργατών.
- Εξουσιοδότηση για άντληση στοιχείων και συνεντεύξεις
- Χρονοδιάγραμμα- πλάνο μελέτης

Εφόσον γίνουν εφικτά τα παραπάνω ακολουθούνται 3 κύρια στάδια ακολουθεί :

- **Προσδιορισμός και αξιολόγηση των Αγαθών που χρήζουν προστασία** (δεδομένα που χειρίζεται το ΠΣ σε συνδυασμό με το λογισμικό και το υλικό του. Ανάλυση μεγέθους καταστροφής των δεδομένων, μεταβολής τους άνευ εξουσιοδότησης, λάθος μετάδοσης τους καθώς επίσης και τα μη διαθέσιμα δεδομένα που μπορεί να υπάρξουν όπως αναλύθηκαν πιο πριν. Όταν συγκεντρωθούν οι απαραίτητες πληροφορίες και τα αποτελέσματα του σταδίου τότε η αποτίμηση "ζημιών" γίνεται από την διοίκηση του οργανισμού και έρχεται σε εφαρμογή το δεύτερο στάδιο)
- **Ανάλυση Επικινδυνότητας** (προσδιορισμός εκάστοτε απειλής και εκτίμηση. Υπολογισμός επικινδυνότητας και τέλος επιβεβαίωση και επικύρωση του βαθμού επικινδυνότητας)
- **Διαχείριση Επικινδυνότητας** (Λίστα προτεινόμενων αντιμέτρων και τα αποτελέσματα τους εφόσον εφαρμοστούν δίνοντας βάση στην επίδρασή τους στο ΠΣ και κατ' επέκταση στον οργανισμό, χρηματικό κόστος και ανθρώπινοι πόροι που θα χρησιμοποιηθούν για την αποτελεσματικότητα του σχεδίου και την μείωση μελλοντικών απειλών – αδυναμιών. Τέλος γίνεται η κατάρτιση σχεδίου ασφαλείας και η εφαρμογή του.)

Επιπλέον, για την διευκόλυνση της ανάλυσης κινδύνων πολλές εταιρείες έχουν αναπτύξει λογισμικά ανάλυσης κινδύνου. Εμείς αναφέρουμε εδώ το Callio Secura το οποίο είναι ένα σύστημα διαχείρισης ασφάλειας πληροφοριακών συστημάτων με έμφαση την συμμόρφωση με το διεθνές στάνταρ BS7799 / ISO 17799.Βασίζεται σε μια δική του μέθοδο για την ανάλυση κινδύνων που είναι σχετικά απλή, βήμα προς βήμα, ώστε να γίνεται εύκολα κατανοητή και να μην απαιτεί ειδικευμένο προσωπικό για την χρήση του.

Καθώς επίσης και το λογισμικό COBRA που χρησιμοποιεί την δική του μέθοδο για ανάλυση κινδύνων, η οποία βοηθάει στην επίτευξη συμμόρφωσης με το διεθνές στάνταρ ISO17799/BS7799. Ένα από τα σημαντικότερα πλεονεκτήματα του είναι η αυτόματη προσαρμογή της ανάλυσης στις συγκεκριμένες ανάγκες του κάθε οργανισμού.

Ολοκληρώνοντας, είναι σημαντικό να θυμίσουμε πως αναφέραμε στα Μοντέλα Διαχείρισης Επικινδυνότητας, το μοντέλο Αντικειμενοστραφούς Προσέγγισης και το μοντέλο TOPM.

Έπειτα από την ανάλυση όλων αυτών κατέληξα στο συμπέρασμα ότι δεν μπορούμε να ξεχωρίσουμε κάποια από τις μεθόδους καθώς και οι τέσσερις έχουν θετικά και αρνητικά στοιχεία.

Η πιο διαδεδομένη και επιτυχημένη σε εφαρμογή μέθοδος είναι η CRAMM καθώς καλύπτει το σύνολο ανάλυσης και διαχείρισης επικινδυνότητας και συνοδεύεται από μια βιβλιοθήκη αντιμέτρων κάτι στο οποίο οι δυο άλλες μέθοδοι SBA, MARION υστερούν. Από την άλλη, είναι αρκετά κοστοβόρα σε σχέση με τις προαναφερθείσες που έχουν σχετικά χαμηλό κόστος και τέλος η CRAMM έχει επίσης, υψηλό κόστος σε ανθρώπινη προσπάθεια καθώς στηρίζεται κυρίως σε υποκειμενικές εκτιμήσεις και τα προτεινόμενα αντίμετρα είναι πολύ γενικά.

Πιστεύω λοιπόν ότι, η επιλογή αυθαίρετα μίας μεθόδου δεν είναι λύση καθώς θεωρώ πως θα πρέπει να λαμβάνονται σοβαρά υπόψη πολλές παράμετροι όπως το κόστος εφαρμογής από άποψη χρόνου, χρημάτων και ανθρώπινης προσπάθειας , η ικανότητα διαχείρισης του συστήματος από το προσωπικό καθώς και τα χαρακτηριστικά και η κουλτούρα του οργανισμού.

ΒΙΒΛΙΟΓΡΑΦΙΑ

1).*ΜΠΟΖΙΟΣ ΕΛ. (2004) "Σημειώσεις Εφαρμοσμένης Ασφάλειας πληροφοριακών συστημάτων"*

2).ΚΑΡΥΔΑ ΜΑΡΙΑ (2010) "Πολιτικές Ασφάλειας Πληροφοριακών Συστημάτων "

3).ΚΑΤΣΙΚΑΣ Κ. ΣΩΚΡΑΤΗΣ " Πολιτικές Ασφάλειας Πληροφοριακών Συστημάτων "

4).ΚΑΤΣΙΚΑΣ ΣΩΚΡΑΤΗΣ "Πολιτικές και Διαχείριση Ασφάλειας , εισαγωγικά θέματα"

5).ΚΟΚΟΛΑΚΗΣ ΣΠ.. "Ανάλυση , αποτίμηση και διαχείριση επικινδυνότητας ΠΣ"

6).Δρ.ΠΑΠΑΝΑΓΙΩΤΟΥ ΚΩΝ..2009 "Προστασία και ασφάλεια υπολογιστικών συστημάτων"

7).ΝΟΜΟΣ 2472/97, "Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα"10-4-1997/ΦΕΚ 50/Τεύχος Α', 1997.

8).ΝΙΚΗΤΑΣ Γ..(2004) "Ανάλυση Κινδύνων Πληροφοριακών Συστημάτων"

9).WAHLGREN G. (1995) ''An object oriented approach to an IT risk management system'', In Information Security - the Next Decade (eds. Ellof J. and S. von Solms), pp.79-86. Proceedings of the 11th International Conference in Information Security, IFIP' 95, Chapman-Hall, London.

10).ELOFF J.H.P., BADENHORST K.P. (1994) ''TOPM: o formal approach to the optimisation of information technology risk management'', Computers & Security, Vol.13, No.5, pp.411-435.