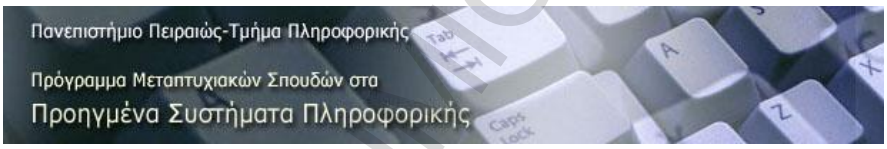
Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής

Πρόγραμμα Μεταπτυχιακών Σπουδών

«Προηγμένα Συστήματα Πληροφορικής»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**Ασφάλεια Πληροφορίας και Ανάλυση Κινδύνων στα Πληροφοριακά Συστήματα- Μελέτη Περίπτωσης με χρήση του EBIOS** **Information Security and Risk Analysis for Information Systems- Case study with the use of EBIOS**
Ονοματεπώνυμο Φοιτητή	**Σάσσαλος Ανδρέας του Ιωάννη**
Αριθμός Μητρώου	**ΜΠΣΠ/ 09009**
Κατεύθυνση	**Δικτυοκεντρικά Πληροφοριακά Συστήματα**
Επιβλέπουσα	**Δέσποινα Πολέμη, Επίκουρος Καθηγήτρια**



Ημερομηνία Παράδοσης **Απρίλιος 2013**

Τριμελής Εξεταστική Επιτροπή

(υπογραφή)	(υπογραφή)	(υπογραφή)
Δέσποινα Πολέμη Επίκουρος Καθηγήτρια	Χρήστος Δουληγέρης Καθηγητής	Παναγιώτης Κοτζανικολάου Λέκτορας

Ευχαριστίες

Θα ήθελα να ευχαριστήσω θερμά την Επίκουρο Καθηγήτρια Κα. Δέσποινα Πολέμη, για την πολύτιμη καθοδήγησή, στήριξη και την άψογη συνεργασία μας κατά τη διάρκεια εκπόνησης της εργασίας. Επίσης, θα ήθελα να ευχαριστήσω τον πολύ καλό φίλο και συνάδελφο Δημήτρη Παρά για την πολύτιμη βοήθειά του. Κλείνοντας θέλω να πω ένα μεγάλο ευχαριστώ στους γονείς μου, την αδερφή μου και τη Σοφία για την υπομονή και την κατανόησή τους όλο αυτό τον καιρό.

Ανδρέας Σάσσαλος

Περίληψη

Οι οργανισμοί που βασίζονται στα πληροφοριακά τους συστήματα για την εκτέλεση τόσο της αποστολής τους όσο και των επιχειρησιακών λειτουργιών τους, αντιμετωπίζουν τον κίνδυνο σοβαρών απειλών, οι οποίες μπορούν να εκμεταλλευθούν γνωστές αλλά και άγνωστες αδυναμίες των συστημάτων αυτών. Μεταξύ των απειλών συγκαταλέγονται στοχευμένες επιθέσεις, διακοπές στη λειτουργία των οργανισμών που οφείλονται σε φυσικές καταστροφές, ανθρώπινα λάθη ή λάθη συστήματος και διαρθρωτικές αδυναμίες. Αυτές οι δυνητικά επιβλαβείς δραστηριότητες μπορούν να θέσουν σε κίνδυνο την εμπιστευτικότητα, ακεραιότητα ή διαθεσιμότητα της πληροφορίας που επεξεργάζεται, αποθηκεύεται ή μεταδίδεται από τα πληροφοριακά συστήματα, με αποτέλεσμα να προκύπτουν αρνητικές επιπτώσεις στον οργανισμό, στις λειτουργίες του, στα αγαθά και στους ανθρώπους του, αλλά και να θέτουν παράλληλα σε κίνδυνο άλλους οργανισμούς ακόμα και εθνικά συμφέροντα.

Οι άνθρωποι σε όλα τα επίπεδα ενός οργανισμού έχουν ένα ρόλο στη διαχείριση των κινδύνων ασφάλειας πληροφορίας που αφορά την αποστολή του οργανισμού, τις επιχειρησιακές λειτουργίες του και τα πληροφοριακά συστήματα που τις υποστηρίζουν. Η διαχείριση του κινδύνου είναι μία ολοκληρωμένη και πολύπλοκη διαδικασία που περιλαμβάνει πολλές δραστηριότητες και λειτουργίες ενός οργανισμού (προγράμματα, επενδύσεις, προϋπολογισμός, νομικά και ζητήματα ασφάλειας). Μία ολοκληρωμένη προσέγγιση για τη διαχείριση του κινδύνου συγκεντρώνει τις καλύτερες αποφάσεις των ατομικών και ομαδικών οργάνων του οργανισμού, που είναι υπεύθυνα για το στρατηγικό σχεδιασμό, την εποπτεία, τη διαχείριση και τις καθημερινές εργασίες του [20].

Η ανάλυση επικινδυνότητας είτε αφορά την ασφάλεια πληροφορίας είτε άλλα είδη κινδύνου θα πρέπει να πραγματοποιείται σε μία συνεχή βάση, διότι αποτελεί το μέσο παροχής της απαραίτητης πληροφορίας σε αυτούς που λαμβάνουν τις αποφάσεις για να κατανοήσουν του παράγοντες που μπορούν να επηρεάσουν αρνητικά τις δραστηριότητες και τα αποτελέσματα αυτών, με στόχο τη λήψη ενημερωμένων αποφάσεων αναφορικά με την έκταση των απαιτούμενων ενεργειών για τη μείωση του κινδύνου. Οι οργανισμοί μπορούν να διενεργούν αναλύσεις επικινδυνότητας κατά τη διάρκεια της ανάπτυξης του κύκλου ζωής των συστημάτων και σε όλα τα επίπεδα της ιεραρχίας διαχείρισης επικινδυνότητας, σύμφωνα με τις αποφάσεις της διοίκησης που αφορούν τη συχνότητα τους και τους απαιτούμενους πόρους [25].

Αυτή η μεταπτυχιακή διατριβή ασχολείται με την ασφάλεια της πληροφορίας και την ανάλυση των κινδύνων που αντιμετωπίζουν τα πληροφοριακά συστήματα των οργανισμών. Αρχικά, μετά από μία σύντομη εισαγωγή, στο κεφάλαιο 2, παρουσιάζεται αναλυτικά το Διεθνές Πρότυπο ISO/IEC 27002:2005 το οποίο θεσπίζει μία σειρά από οδηγίες και βέλτιστες πρακτικές για τη διαχείριση της ασφάλειας πληροφορίας. Εν συνέχεια, στο κεφάλαιο 3, παρουσιάζεται η διαχείριση επικινδυνότητας στα πληροφοριακά συστήματα και ορισμένες από τις κυριότερες και πιο χαρακτηριστικές μεθοδολογίες που χρησιμοποιούνται στην ανάλυση κινδύνων των πληροφοριακών συστημάτων. Στο κεφάλαιο 4, παρουσιάζεται αναλυτικά η μεθοδολογία EBIOS και το αντίστοιχο εργαλείο μέσα από τη μελέτη ανάλυσης κινδύνων σε μία Βιβλιοθήκη Πανεπιστημίου. Τέλος, στο κεφάλαιο 5, αναφέρονται τα συμπεράσματα αυτής της μελέτης και ορισμένες προτάσεις για μελλοντική επέκταση της μελέτης και περαιτέρω έρευνα.

Λέξεις κλειδιά: Ασφάλεια πληροφορίας, Ανάλυση κινδύνων, Μεθοδολογίες και εργαλεία ανάλυσης κινδύνων, EBIOS.

Περιεχομενα

ΠΕΡΙΕΧΟΜΕΝΑ ΕΙΚΟΝΩΝ

ΠΕΡΙΕΧΟΜΕΝΑ ΠΙΝΑΚΩΝ

1. Εισαγωγή

Η πληροφορία αποτελεί ένα σημαντικό αγαθό για κάθε οργανισμό και ως τέτοιο θα πρέπει να προστατεύεται καταλλήλως. Λόγω της αυξανόμενης διασυνδεσιμότητας στο επιχειρηματικό περιβάλλον όμως, η πληροφορία εκτίθεται σε ένα ολοένα αυξανόμενο αριθμό και μία ευρύτερη ποικιλία απειλών και τρωτών σημείων. Ασφάλεια πληροφορίας είναι η προστασία της πληροφορίας από ένα ευρύ φάσμα απειλών με στόχο τη διασφάλιση της συνέχειας της επιχειρηματικής δραστηριότητας, την ελαχιστοποίηση του επιχειρηματικού κινδύνου και τη μεγιστοποίηση της απόδοσης των επενδύσεων [5]. Η ασφάλεια επιτυγχάνεται με την εφαρμογή ενός κατάλληλου συνόλου ελέγχου, συμπεριλαμβανομένων των πολιτικών, διαδικασιών, οργανωτικών δομών, καθώς και των λειτουργιών του λογισμικού και υλικού. Οι έλεγχοι αυτοί πρέπει να δημιουργηθούν, εφαρμοστούν, παρακολουθηθούν, αξιολογηθούν και βελτιωθούν, όπου αυτό είναι αναγκαίο για την εξασφάλιση της πλήρωσης των ειδικών επιχειρηματικών και στόχων ασφάλειας του οργανισμού. Αυτό θα πρέπει να επιτευχθεί σε συνδυασμό και με άλλες μεθόδους διοίκησης της επιχείρησης.

Σημαντικά επιχειρηματικά αγαθά μαζί με την πληροφορία είναι τα συστήματα, τα δίκτυα και οι διαδικασίες υποστήριξης. Ο καθορισμός, η επίτευξη, η διατήρηση και η βελτίωση της ασφάλειας της πληροφορίας αποτελούν απαραίτητα στοιχεία για την απόκτηση ανταγωνιστικού πλεονεκτήματος, κερδοφορίας, νομικής συμμόρφωσης και εμπορικής εικόνας. Οι οργανισμοί, τα πληροφοριακά τους συστήματα καθώς και τα δίκτυα αυτών, βρίσκονται αντιμέτωποι με ένα ευρύ φάσμα απειλών κατά της ασφάλειάς τους, όπως είναι η απάτη με τη βοήθεια υπολογιστών, η κατασκοπεία, οι βανδαλισμοί, η φωτιά, οι πλημμύρες. Επιθέσεις από κακόβουλο λογισμικό, *"hacking"*, άρνηση παροχής υπηρεσιών γίνονται ολοένα και συχνότερες, πιο φιλόδοξες και πιο εξελιγμένες.

Η ασφάλεια της πληροφορίας είναι υψίστης σημασίας τόσο στο δημόσιο όσο και στον ιδιωτικό τομέα, καθώς και στις κρίσιμες υποδομές και μπορεί να λειτουργήσει ως καταλύτης, π.χ. για την επίτευξη της ηλεκτρονικής διακυβέρνησης ή του ηλεκτρονικού επιχειρήν, αποφεύγοντας ή μειώνοντας τους σχετικούς κινδύνους. Η δαισυνδεσιμότητα μεταξύ δημόσιων και ιδιωτικών δικτύων, καθώς και η ανταλλαγή πληροφοριακών πόρων, αυξάνουν τη δυσκολία του ελέγχου πρόσβασης. Η διάδοση των κατανεμημένων υπολογιστικών συστημάτων έχει ως αποτέλεσμα την αδυναμία ενός αποτελεσματικού κεντρικού, ειδικού ελέγχου. Τα περισσότερα πληροφοριακά συστήματα δεν έχουν σχεδιαστεί με τέτοιο τρόπο ώστε να είναι ασφαλή. Η ασφάλεια που μπορεί να επιτευχθεί με τεχνικά μέσα είναι περιορισμένη και θα πρέπει να υποστηρίζεται από κατάλληλες διαδικασίες και διοίκηση. Ο προσδιορισμός των κατάλληλων ελέγχων που θα πρέπει να εφαρμοστούν απαιτεί προσεκτικό σχεδιασμό και προσοχή στη λεπτομέρεια [1]. Η διαχείριση της ασφάλειας της πληροφορίας απαιτεί, κατ' ελάχιστο, τη συμμετοχή όλων των εργαζομένων ενός οργανισμού, ενώ μπορεί να απαιτείται και η συμμετοχή μετόχων, προμηθευτών, πελατών ή και τρίτων, καθώς και η ανάγκη ειδικών συμβουλευτικών οργανισμών.

Είναι ουσιώδες ένας οργανισμός να μπορεί να προσδιορίσει τις απαιτήσεις ασφάλειάς του. Μπορούν να εντοπισθούν τρεις κύριες πηγές απαιτήσεων ασφάλειας:

1. Μία πηγή απορρέει από την αξιολόγηση των κινδύνων ενός οργανισμού, λαμβάνοντας υπόψη τη συνολική επιχειρηματική στρατηγική και στόχους. Μέσα από την παραπάνω διαδικασία αναγνωρίζονται οι απειλές των αγαθών, αξιολογούνται η ευπάθεια και η πιθανότητα εμφάνισής των και γίνεται μία εκτίμηση των πιθανών επιπτώσεων.
2. Μία άλλη πηγή είναι οι νομικές, κανονιστικές, ρυθμιστικές και συμβατικές απαιτήσεις που ένας οργανισμός, οι εμπορικοί εταίροι, ανάδοχοι και πάροχοι υπηρεσιών θα πρέπει να πληρούν, καθώς επίσης και το κοινωνικό-πολιτιστικό περιβάλλον τους.
3. Τέλος, είναι το συγκεκριμένο σύνολο στόχων, αρχών και επιχειρηματικών απαιτήσεων για την επεξεργασία των πληροφοριών που ένας οργανισμός έχει αναπτύξει για την υποστήριξη των λειτουργιών του.

Οι απαιτήσεις ασφάλειας προκύπτουν μετά από μεθοδική αξιολόγηση των κινδύνων. Θα πρέπει να σταθμισθούν οι δαπάνες για ελέγχους σε σχέση με την πιθανή ζημία της επιχείρησης ως αποτέλεσμα αδυναμιών ασφάλειας. Τα αποτελέσματα της αξιολόγησης θα βοηθήσουν στην καθοδήγηση και προσδιορισμό των απαραίτητων ενεργειών διοίκησης, τις προτεραιότητες στη διαχείριση κινδύνων

ασφάλειας πληροφορίας, καθώς και εφαρμογή επιλεγμένων ελέγχων για την προστασία από τους παραπάνω κινδύνους. Η αξιολόγηση των κινδύνων είναι μία διαδικασία η οποία θα πρέπει να επαναλαμβάνεται κατά διαστήματα για τον εντοπισμό τυχόν αλλαγών που θα μπορούσαν να επηρεάσουν τα αποτελέσματά της.

Από τη στιγμή που οι απαιτήσεις ασφάλειας και οι κίνδυνοι έχουν εντοπισθεί, και έχουν ληφθεί οι αποφάσεις για την αντιμετώπισή τους, θα πρέπει να επιλεγούν και εφαρμοσθούν οι κατάλληλοι έλεγχοι ώστε να διασφαλισθεί ότι οι κίνδυνοι θα περιορισθούν σε ένα αποδεκτό επίπεδο. Οι έλεγχοι μπορούν είτε να βασίζονται σε συγκεκριμένες νομοθετικές απαιτήσεις, είτε σε κάποιες κοινές πρακτικές ασφάλειας. Σε κάθε περίπτωση πάντως, θα πρέπει να υπάρχει συσχέτιση των ελέγχων με τους ιδιαίτερους κινδύνους που αντιμετωπίζει ο κάθε οργανισμός.

Η εφαρμογή της ασφάλειας της πληροφορίας σε έναν οργανισμό με επιτυχία, μπορεί να επηρεασθεί από κάποιους κρίσιμους παράγοντες, όπως:

i. Πολιτικές ασφάλειας, στόχοι και δραστηριότητες που αντανακλούν σε αυτούς,
ii. Μία προσέγγιση και ένα πλαίσιο για την εφαρμογή, διατήρηση, παρακολούθηση και βελτίωση της ασφάλειας πληροφορίας που είναι συνεπής με την κουλτούρα του οργανισμού,
iii. Στήριξη και δέσμευση από όλα τα επίπεδα της διοίκησης,
iv. Σωστή κατανόηση των απαιτήσεων ασφάλειας, της εκτίμησης και διαχείρισης του κινδύνου,
v. Ουσιαστική προώθηση της ασφάλειας της πληροφορίας στα διευθυντικά στελέχη, εργαζόμενους και τρίτους για την επίτευξη ευαισθητοποίησης,
vi. Κατευθυντήριες οδηγίες όσον αφορά τις πολιτικές ασφάλειας και τα πρότυπα στους παραπάνω,
vii. Πρόβλεψη για τη χρηματοδότηση δραστηριοτήτων διαχείρισης ασφάλειας πληροφοριών,
viii. Παροχή κατάλληλης ενημέρωσης, κατάρτισης και εκπαίδευσης,
ix. Θέσπιση αποτελεσματικών διαδικασιών διαχείρισης περιστατικού ασφαλείας,
x. Εφαρμογή ενός συστήματος μέτρησης για την αξιολόγηση της απόδοσης με ταυτόχρονη επανατροφοδότηση για τη βελτίωση της διαχείρισης ασφάλειας πληροφορίας.

2. Το Διεθνές Πρότυπο ISO/IEC 27002:2005

2.1 Πεδίο εφαρμογής – δομή προτύπου

Το Διεθνές Πρότυπο ISO/IEC 27002:2005 "Information technology – Security techniques – Code of practice for information security management" θεσπίζει οδηγίες και γενικές αρχές για την έναρξη, υλοποίηση, συντήρηση και βελτίωση της διαχείρισης της ασφάλειας της πληροφορίας μέσα σε ένα οργανισμό. Οι στόχοι και οι έλεγχοι που προτείνει το πρότυπο πρέπει να εφαρμοστούν ώστε να πληρούν τις απαιτήσεις που προσδιορίζονται από την εκτίμηση των κινδύνων. Το Διεθνές Πρότυπο μπορεί να λειτουργήσει ως μία πρακτική καθοδήγηση για την ανάπτυξη προτύπων ασφάλειας και αποτελεσματικών πρακτικών διοίκησης και κατ' επέκταση να οδηγήσει στην εμπιστοσύνη στις εσωτερικές δραστηριότητες ενός οργανισμού [15].

Το πρότυπο περιλαμβάνει έντεκα (11) σημεία ελέγχου ασφάλειας, τα οποία με τη σειρά τους περιέχουν τριάντα εννέα (39) βασικές κατηγορίες καθώς και μία εισαγωγή που αφορά την εκτίμηση και αντιμετώπιση των κινδύνων:

1. Πολιτική Ασφάλειας – Π.Α. (1)
2. Οργάνωση Ασφάλειας της Πληροφορίας (2)
3. Διαχείριση Αγαθών (2)
4. Ασφάλεια Προσωπικού (3)
5. Ασφάλεια από φυσικές και περιβαλλοντικές καταστροφές (2)
6. Διαχείριση Τηλεπικοινωνιών και Λειτουργιών (10)
7. Έλεγχος πρόσβασης (7)
8. Προμήθεια, Ανάπτυξη και Συντήρηση Πληροφοριακών Συστημάτων (6)
9. Διαχείριση Περιστατικών Ασφάλειας (2)
10. Διαχείριση Συνέχειας Επιχειρηματικής Δραστηριότητας (1)
11. Συμμόρφωση (3).

Κάθε βασική κατηγορία περιλαμβάνει με τη σειρά της ένα στόχο ελέγχου, όπου δηλώνεται τι πρέπει να επιτευχθεί και έναν ή περισσότερους ελέγχους που πρέπει να γίνουν ώστε να επιτευχθεί αυτός ο στόχος. Η περιγραφή του κάθε ελέγχου έχει συγκεκριμένη δομή η οποία αποτελείται από (α) τον καθορισμό του μέσα από μία ειδική δήλωση ώστε να ικανοποιείται ο στόχος του, (β) οδηγίες, οι οποίες παρέχουν λεπτομερέστερη πληροφορία ώστε να υποστηρίζεται η εφαρμογή του και να πληρούνται οι απαιτήσεις που έχουν τεθεί και (γ) λοιπή-συμπληρωματική πληροφορία που θα πρέπει να ληφθεί υπόψη, όπως νομικά ζητήματα και αναφορές σε άλλα πρότυπα[5] [14][15] [16].

2.2 Ανάλυση και αντιμετώπιση κινδύνου

Οι αξιολογήσεις των κινδύνων θα πρέπει πρωταρχικά να εντοπίζουν, ποσοτικοποιούν και ιεραρχούν τους κινδύνους, με κριτήριο πάντα την αποδοχή του κινδύνου και τους στόχους του οργανισμού. Τα αποτελέσματα θα πρέπει να καθοδηγούν και καθορίζουν κατάλληλες δράσεις διοίκησης και να θέτουν προτεραιότητες διαχείρισης των κινδύνων και να εφαρμόζουν επιλεγμένους ελέγχους προς αντιμετώπισή τους. Η διαδικασία της εκτίμησης κινδύνων και της εφαρμογής ελέγχων δύναται να εκτελεσθεί αρκετές φορές ώστε να καλυφθούν τα διάφορα τμήματα του οργανισμού ή τα διαφορετικά πληροφοριακά συστήματα. Η εκτίμηση θα πρέπει να περιλαμβάνει μία συστηματική προσέγγιση του μεγέθους του κινδύνου (**ανάλυση κινδύνου**), καθώς και μία σύγκριση με τα κριτήρια του καθορισμού της σημασίας των κινδύνων (**αξιολόγηση κινδύνου**).

Η παραπάνω διαδικασία της εκτίμησης των κινδύνων θα πρέπει επίσης να διεξάγεται κατά τακτά διαστήματα, ώστε να εντοπίζονται τυχόν αλλαγές στις απαιτήσεις ασφάλειας και την κατάσταση των κινδύνων που αφορούν τα αγαθά, τις απειλές, τις τρωτότητες, τις επιπτώσεις τους. Οι εκτιμήσεις θα πρέπει να ενεργούνται με συγκεκριμένες μεθόδους που να παράγουν συγκρίσιμα και αναπαραγωγίσιμα αποτελέσματα. Περαιτέρω, θα πρέπει να είναι ξεκάθαρα καθορισμένο το πεδίο εφαρμογής της παραπάνω διαδικασίας και αν είναι δυνατόν να συσχετίζεται με αξιολόγηση κινδύνων

άλλων τομέων. Το πεδίο εφαρμογής μπορεί να αφορά ολόκληρο τον οργανισμό, τμήματα αυτού, ένα μεμονωμένο πληροφοριακό σύστημα, συγκεκριμένα κομμάτια του συστήματος ή ακόμα και σε υπηρεσίες, όπου αυτό είναι εφικτό, ρεαλιστικό και χρήσιμο.

Προτού την αντιμετώπιση ενός κινδύνου, ο οργανισμός θα πρέπει να αποφασίσει και καθορίσει τα κριτήρια βάση των οποίων οι κίνδυνοι μπορούν να γίνουν αποδεκτοί ή όχι. Για κάθε κίνδυνο που εντοπίζεται από τη διαδικασία εκτίμησης, θα πρέπει να ληφθεί μία απόφαση αντιμετώπισής του, η οποία μπορεί να περιλαμβάνει:

α) Εφαρμογή κατάλληλων ελέγχων για τη μείωση κινδύνων,
β) Αποδοχή του κινδύνου εν γνώσει του οργανισμού εφόσον ικανοποιείται η Πολιτική Ασφάλειας του οργανισμού και πληρούνται τα κριτήρια που έχει θέσει,
γ) Αποφυγή των κινδύνων μη επιτρέποντας τις ενέργειες που θα μπορούσαν να τους προκαλέσουν και
δ) Μεταφορά των συναφών κινδύνων σε τρίτους όπως ασφαλιστές ή προμηθευτές.

Οι έλεγχοι θα πρέπει να διασφαλίζουν ότι οι κίνδυνοι μειώνονται σε ένα αποδεκτό επίπεδο, λαμβάνοντας όμως υπόψη:

α) Τις απαιτήσεις και περιορισμούς της εθνικής και διεθνούς νομοθεσίας και των κανονισμών,
β) Τους στόχους του οργανισμού,
γ) Τις λειτουργικές απαιτήσεις και περιορισμούς,
δ) Τα κόστη εφαρμογής και λειτουργίας σε σχέση με τους κινδύνους που μειώνονται, παραμένοντας αναλογικά πάντα στα επίπεδα του οργανισμού,
ε) Την ανάγκη εξισορρόπησης της επένδυσης για την εφαρμογή και εκτέλεση ελέγχων σε σχέση με την ζημία που θα προκληθεί σε περίπτωση αποτυχίας ασφάλειας.

Θα πρέπει να τονισθεί ότι οι έλεγχοι σε θέματα ασφάλειας πληροφορίας θα πρέπει να λαμβάνονται υπόψη κατά το στάδιο του σχεδιασμού, του προσδιορισμού των απαιτήσεων και προδιαγραφών των συστημάτων, σε αντίθετα περίπτωση το αποτέλεσμα θα είναι επιπρόσθετα κόστη, λιγότερο αποτελεσματικές λύσεις, και στη χειρότερη περίπτωση, αδυναμία επίτευξης επαρκούς ασφάλειας. Τέλος, θα πρέπει να γίνει κατανοητό ότι κανένα σύνολο ελέγχων δεν μπορεί να επιτύχει την απόλυτη ασφάλεια, και πως θα πρέπει να εφαρμοστούν επιπλέον μέτρα διαχείρισης για την παρακολούθηση, αξιολόγηση και βελτίωση της αποδοτικότητας και αποτελεσματικότητας των ελέγχων για τη στήριξη των στόχων του οργανισμού.

2.3 Πολιτική Ασφάλειας Πληροφορίας

Η Πολιτική Ασφάλειας της Πληροφορίας ενός οργανισμού έχει ως στόχο την εναρμόνιση της διοίκησης σε θέματα ασφάλειας της πληροφορίας με τις απαιτήσεις αυτού, την κείμενη νομοθεσία και τους κανονισμούς. Η διοίκηση θα πρέπει να θέσει ξεκάθαρα την πολιτική ασφάλειας που θα ακολουθήσει σύμφωνα πάντα με τους επιχειρηματικούς στόχους του οργανισμού και να επιδείξει τη στήριξη και δέσμευσή της σε αυτή. Αυτό γίνεται μέσω ενός **εγγράφου** (**document**) το οποίο εγκρίνεται από τη διοίκηση, υπογράφεται και κοινοποιείται σε όλους τους εργαζομένους και εξωτερικούς συνεργάτες. Το έγγραφο , το οποίο αποτελεί ουσιαστικά και μία δέσμευση της διοίκησης θα πρέπει να περιλαμβάνει:

1. Έναν ορισμό της ασφάλειας πληροφοριών, τους αντικειμενικούς της στόχους, το πεδίο εφαρμογής και τη σημασία της ασφάλειας ως ένα καθοριστικό μηχανισμό για την ανταλλαγή πληροφορίας.
2. Μία δήλωση των προθέσεων της διοίκησης, υποστηρίζοντας τις αρχές της ασφάλειας, σύμφωνα πάντα με την επιχειρηματική στρατηγική.
3. Ένα πλαίσιο για τον καθορισμό ελέγχων, συμπεριλαμβανομένης και της εκτίμησης και διαχείρισης κινδύνου.
4. Μία σύντομη επεξήγηση των πολιτικών, αρχών, προτύπων ασφάλειας και απαιτήσεων συμμόρφωσης με: α) τη νομοθεσία, τους κανονισμούς και τις συμβάσεις, β) θέματα εκπαίδευσης, κατάρτισης και ευαισθητοποίησης, γ) τη διαχείριση συνέχειας επιχειρηματικής δραστηριότητας, δ) τις συνέπειες από παραβιάσεις της πολιτικής ασφάλειας.

5. Καθορισμό γενικών και ειδικών καθηκόντων, συμπεριλαμβανομένης της καταγραφής των περιστατικών ασφαλείας.
6. Τεκμηρίωση της πολιτικής μέσω αναφορών σε πιο λεπτομερείς διαδικασίες ασφάλειας για εξειδικευμένα πληροφοριακά συστήματα ή κανόνες ασφάλειας στους οποίους οι χρήστες θα πρέπει να συμμορφώνονται.

Η πολιτική ασφάλειας θα πρέπει να επανεξετάζεται σε προκαθορισμένα χρονικά διαστήματα ή όταν συμβαίνουν σημαντικές αλλαγές, ώστε να διασφαλιστεί η καταλληλότητα, επάρκεια και αποτελεσματικότητά της. Θα πρέπει να περιλαμβάνει μία εκτίμηση των δυνατοτήτων που υπάρχουν για βελτίωση και μία προσέγγιση διοίκησης ως απάντηση στις αλλαγές του περιβάλλοντος του οργανισμού, των συνθηκών της επιχείρησης, των νομικών και τεχνικών προϋποθέσεων. Παράλληλα, θα λαμβάνονται υπόψη η κατάσταση των αποτρεπτικών και διορθωτικών ενεργειών, η απόδοση των διαδικασιών και η συμμόρφωση με την πολιτική ασφάλειας, συνήθειες που σχετίζονται με τις απειλές και τρωτότητες, αναφορές περιστατικών και συστάσεις από συνεργαζόμενους φορείς. Σημαντική κρίνεται η τήρηση αρχείου με τους παραπάνω ελέγχους.

2.4 Οργάνωση Ασφάλειας Πληροφορίας

2.4.1 Εσωτερική οργάνωση

Θα πρέπει να εφαρμοσθεί ένα πλαίσιο διαχείρισης της ασφάλειας πληροφορίας μέσα στον οργανισμό. Πρόσθετα, η διοίκηση θα πρέπει να εγκρίνει το κείμενο της πολιτικής, να αναθέσει καθήκοντα και να συντονίσει και επανεξετάσει το κατά πόσο αυτή εφαρμόζεται. Εάν κριθεί απαραίτητο, θα πρέπει να αναζητηθεί πηγή βοηθείας από ειδικούς σε θέματα ασφάλειας, συνάπτοντας συνεργασίες με εξωτερικούς συνεργάτες και σχετικούς φορείς, ώστε να συμβαδίζει με τις νέες τάσεις, να παρακολουθεί τα πρότυπα, τις μεθόδους αξιολόγησης, παρέχοντας κατ' αυτόν τον τρόπο μία διεπιστημονική προσέγγιση στην αντιμετώπιση περιστατικών ασφαλείας. Το πλαίσιο διαχείρισης της ασφάλειας υλοποιείται μέσω των παρακάτω ενεργειών:

1. *Δέσμευση της Διοίκησης σε θέματα Ασφάλειας:* Η Διοίκηση θα πρέπει να υποστηρίζει ενεργά την ασφάλεια εντός του Οργανισμού, με σαφείς κατευθύνσεις, την έμπρακτη δέσμευση στους στόχους, την σαφή κατανομή καθηκόντων και ευθυνών, τη δέσμευση των απαιτούμενων πόρων και την προώθηση της ευαισθητοποίησης σε θέματα ασφάλειας μέσω ειδικών προγραμμάτων.
2. *Συντονισμός:* Οι ενέργειες που σχετίζονται με την ασφάλεια πολύ πιθανό να πρέπει να γίνουν από διαφορετικά τμήματα του Οργανισμού και γι' αυτό το λόγο θα πρέπει να είναι συντονισμένες. Μέσω του συντονισμού επιτυγχάνεται η συμμόρφωση στην πολιτική ασφαλείας, ενώ εντοπίζονται και αντιμετωπίζονται περιπτώσεις μη-συμμόρφωσης, εγκρίνονται και υλοποιούνται διαδικασίες και μεθοδολογίες όπως εκτίμηση κινδύνου και κατηγοριοποίηση πληροφορίας, εντοπίζονται σημαντικές αλλαγές σε απειλές και η έκθεση του οργανισμού σε αυτές, αξιολογείται η επάρκεια των ελέγχων κ.α.
3. *Ανάθεση Αρμοδιοτήτων:* Η ανάθεση των αρμοδιοτήτων όσον αφορά τα θέματα ασφάλειας θα πρέπει να γίνεται σύμφωνα με αυτά που προβλέπει η πολιτική ασφάλειας. Οι αρμοδιότητες για την προστασία των αγαθών θα πρέπει να ορίζονται με σαφήνεια, και όπου απαιτείται να υπάρχει λεπτομερέστερη καθοδήγηση. Στο πλαίσιο αυτής της διαδικασίας θα πρέπει να καθορίζονται με σαφήνεια τα αγαθά που σχετίζονται με κάθε επιμέρους σύστημα, για κάθε αγαθό ή για την εκτέλεση κάθε διαδικασίας ασφάλειας θα πρέπει να ορίζεται υπεύθυνος και οι λεπτομέρειες των καθηκόντων του θα πρέπει να είναι τεκμηριωμένες, και τέλος, θα πρέπει να ορίζονται με σαφήνεια και να είναι πλήρως τεκμηριωμένα τα επίπεδα εξουσιοδότησης.
4. *Διαδικασία εξουσιοδότησης για χρήση νέων υπολογιστικών συστημάτων:* Για τη χρήση κάθε νέου υπολογιστικού συστήματος θα πρέπει να υπάρχει κατάλληλη διαχείριση της εξουσιοδότησης χρηστών. Όπου αυτό είναι απαραίτητο, θα πρέπει να ελέγχεται ότι υλικό και λογισμικό είναι συμβατά με τα υπόλοιπα εξαρτήματα. Τέλος, η χρήση προσωπικών ή ιδιωτικών μέσων όπως φορητοί υπολογιστές, προσωπικοί υπολογιστές και συσκευές χειρός, τα οποία χρησιμοποιούνται

στην επεξεργασία επιχειρηματικής πληροφορίας, δύναται να δημιουργήσουν νέες τρωτότητες, και γι' αυτό το λόγο πρέπει να γίνονται έλεγχοι εντοπισμού τους.

5. <u>Συμβάσεις εμπιστευτικότητας:</u> Οι απαιτήσεις για εμπιστευτικότητα των δεδομένων του Οργανισμού θα πρέπει να εντοπισθούν, καταγραφούν και να επανεξετάζονται σε τακτά διαστήματα. Προς αυτή την κατεύθυνση θα πρέπει να καθορισθεί ποια πληροφορία είναι εμπιστευτική, η αναμενόμενη διάρκεια μίας σύμβασης, καθώς και οι περιπτώσεις στις οποίες η εμπιστευτικότητα τηρείται επ' αόριστο, οι ενέργειες που πρέπει να γίνουν με τη λήξη μίας σύμβασης, οι υποχρεώσεις των υπογραφόντων μερών για την αποφυγή αποκάλυψης απόρρητης πληροφορίας, θέματα πνευματικής ιδιοκτησίας, εμπορικών μυστικών και πως αυτά σχετίζονται με την προστασία εμπιστευτικής πληροφορίας, διαδικασίες αναφοράς αποκάλυψης ή παραβιάσεων εμπιστευτικής πληροφορίας, όροι επιστροφής ή καταστροφής της πληροφορίας σε περίπτωση διακοπής της σύμβασης και αναμενόμενες ενέργειες σε περίπτωση αθέτησης των όρων της σύμβασης.
6. <u>Επικοινωνία με αρμόδιες αρχές:</u> Οι Οργανισμοί θα πρέπει να διαθέτουν διαδικασίες μέσω των οποίων θα καθορίζεται πότε και με ποιες αρχές (αστυνομικές, πυροσβεστική υπηρεσία, εποπτικές αρχές) θα έρχονται σε επικοινωνία, και μέσα σε ένα εύλογο χρονικό διάστημα, θα αναφέρουν συμβάντα στα οποία υπάρχει υποψία έκνομων ενεργειών. Μπορεί, επίσης, να απαιτείται η συνδρομή με τρίτους (όπως πάροχοι τηλεπικοινωνιών και υπηρεσιών διαδικτύου). Χρήσιμη, επίσης, είναι και η επικοινωνία με ρυθμιστικούς φορείς, για την πρόβλεψη και προετοιμασία επικείμενων αλλαγών στη νομοθεσία ή στους κανονισμούς, που θα πρέπει να ενσωματωθούν από τον Οργανισμό. Τέλος, στα παραπάνω θα πρέπει να συμπεριληφθούν επιχειρήσεις κοινής ωφέλειας, υπηρεσίες έκτακτης ανάγκης, υγείας και ασφάλειας.
7. <u>Επικοινωνία με ομάδες ειδικού ενδιαφέροντος:</u> Πρέπει να υπάρχει επικοινωνία με ειδικούς-επιστήμονες για θέματα ασφάλειας. Τα οφέλη αυτής της επικοινωνίας είναι πολλαπλά, όπως απόκτηση γνώσης των βέλτιστων πρακτικών και συνεχής ενημέρωση σε θέματα ασφάλειας, έγκαιρη λήψη προειδοποιήσεων απέναντι σε επιθέσεις και τρωτότητες, πρόσβαση σε εξειδικευμένες συμβουλές, ανταλλαγή πληροφορίας που αφορά νέες τεχνολογίες, προϊόντα ή απειλές.
8. <u>Ανεξάρτητος έλεγχος:</u> Η προσέγγιση του Οργανισμού σε θέματα ασφάλειας (δηλαδή, στόχοι ελέγχου, πολιτικές, λειτουργίες και διαδικασίες) θα πρέπει να ελέγχεται και αναθεωρείται ανεξάρτητα από τα προγραμματισμένα διαστήματα, ή όταν παρουσιάζονται σημαντικές αλλαγές. Ο ανεξάρτητος έλεγχος θα πρέπει να ξεκινάει από την διοίκηση και να ανατίθεται σε άτομα ανεξάρτητα της περιοχής που ελέγχεται. Η διαδικασία αυτή μπορεί να περιλαμβάνει συνεντεύξεις σε μέλη της διοίκησης, έλεγχο των αναφορών, αναθεώρηση της πολιτικής ασφάλειας.

2.4.2 Εξωτερικοί συνεργάτες

Το επίπεδο ασφαλείας των πληροφοριακών συστημάτων του Οργανισμού δεν πρέπει να μειώνεται όταν γίνεται χρήση προϊόντων ή υπηρεσιών από εξωτερικούς συνεργάτες. Οποιαδήποτε πρόσβαση στα ΠΣ του Οργανισμού από τρίτους θα πρέπει να είναι πλήρως ελεγχόμενη. Όταν υπάρχει απαίτηση για συνεργασία με τρίτους, για την οποία είναι απαραίτητη η πρόσβαση στα ΠΣ του Οργανισμού, πρέπει να εκπονείται ανάλυση και εκτίμηση κινδύνου για τον προσδιορισμό των επιπτώσεων στην ασφάλεια και κατάλληλων μέτρων προστασίας. Τα απαιτούμενα μέτρα ασφαλείας πρέπει να συμφωνούνται και να καταγράφονται σε συμφωνία με τον εξωτερικό συνεργάτη.

1. <u>Εντοπισμός κινδύνων από εξωτερικούς συνεργάτες:</u> Οι κίνδυνοι που υπόκεινται οι πληροφορίες ή τα ΠΣ του Οργανισμού και προέρχονται από εξωτερικούς συνεργάτες θα πρέπει να καταγράφονται και προτού δοθεί πρόσβαση πρέπει να υλοποιούνται όλα τα απαιτούμενα μέτρα ασφαλείας. Θα πρέπει να λαμβάνονται υπόψη ζητήματα, όπως σε ποια ΠΣ αποκτούν πρόσβαση οι εξωτερικοί συνεργάτες, ο τρόπος πρόσβασης (δηλαδή, φυσική πρόσβαση στα γραφεία, στα δωμάτια υπολογιστών και στα αρχεία, πρόσβαση στις βάσεις δεδομένων, απομακρυσμένη πρόσβαση), η αξία, η ευαισθησία και η κρισιμότητα της πληροφορίας για τον Οργανισμό, το προσωπικό των εξωτερικών συνεργατών που έχει πρόσβαση, πώς γίνεται η αυθεντικοποίησή τους, τα διάφορα μέσα που χρησιμοποιούνται κατά την αποθήκευση, επεξεργασία και ανταλλαγή πληροφορίας,

νομικές και κανονιστικές απαιτήσεις και άλλες συμβατικές υποχρεώσεις που πρέπει να ληφθούν υπόψη, καθώς και πώς επηρεάζονται τα συμφέροντα άλλων ενδιαφερομένων από αυτές τις ρυθμίσεις.

2. <u>Ασφάλεια κατά την συναλλαγή με τους πελάτες:</u> Όλες οι απαιτήσεις ασφάλειας θα πρέπει να ικανοποιηθούν προτού επιτραπεί η πρόσβαση από πελάτες στην πληροφορία ή τα αγαθά των ΠΣ του Οργανισμού. Γι' αυτό το λόγο θα πρέπει να λαμβάνονται υπόψη, κατά περίπτωση πάντα, οι παρακάτω όροι:
   α) Προστασία αγαθών, συμπεριλαμβάνοντας, διαδικασίες προστασίας των ΠΣ του Οργανισμού, διαδικασίες για την εξακρίβωση απώλειας ή τροποποίησης δεδομένων, διασφάλιση της ακεραιότητας και περιορισμοί στην αντιγραφή και αποκάλυψη πληροφορίας.
   β) Περιγραφή του προϊόντος ή της υπηρεσίας που θα παρασχεθεί.
   γ) Τους διαφορετικούς λόγους, απαιτήσεις και οφέλη από την πρόσβαση των πελατών.
   δ) Πολιτική ελέγχου πρόσβασης, και μεταξύ άλλων, μεθόδους περιορισμένης πρόσβασης, έλεγχος και χρήση μοναδικών αναγνωριστικών χρήστη, δικαιώματα χρηστών, ανάκληση δικαιωμάτων και διακοπή σύνδεσης μεταξύ των συστημάτων.
   ε) Ρυθμίσεις για αναφορά, ειδοποιήσεις και έρευνα σε περίπτωση ανακριβειών, περιστατικών και κενών ασφαλείας.
   ς) Περιγραφή κάθε υπηρεσίας που θα είναι διαθέσιμη.
   ζ) Καθορισμός του επιδιωκόμενου αποτελέσματος και των μη αποδεκτών επιπέδων υπηρεσιών.
   η) Δικαιώματα παρακολούθησης και αναστολής κάθε δραστηριότητας που σχετίζεται με τα αγαθά του οργανισμού.
   θ) Υποχρεώσεις κατ' αντιστοιχία του οργανισμού και των πελατών.
   ι) Ευθύνες σε σχέση με νομικά ζητήματα, όπως νομοθεσία περί προστασίας δεδομένων, ειδικά σε περιπτώσεις όπου η συμφωνία περιλαμβάνει συνεργασία με πελάτες άλλων χωρών όπου υπάρχει διαφορετική εθνική νομοθεσία.
   ια) Δικαιώματα και εκχώρηση πνευματικής ιδιοκτησίας, και προστασία κάθε συνεργατικής εργασίας.
3. <u>Ασφάλεια κατά τη σύναψη συμβολαίων με τρίτους:</u> Συμβόλαια με τρίτους που προβλέπουν την πρόσβαση, την επεξεργασία, την επικοινωνία ή την διαχείριση της πληροφορίας ή των ΠΣ του οργανισμού, ή την προσθήκη προϊόντων και υπηρεσιών θα πρέπει να ικανοποιούν όλες τις απαιτήσεις ασφάλειας. Για την κάλυψη των απαιτήσεων ασφαλείας θα πρέπει να περιλαμβάνονται στη συμφωνία οι παρακάτω όροι:
   α) Η πολιτική ασφάλειας.
   β) Έλεγχοι για: τις διαδικασίες προστασίας των αγαθών του οργανισμού, την απαίτηση μηχανισμών φυσικής προστασίας, την προστασία από κακόβουλο λογισμικό, τη διασφάλιση επιστροφής ή καταστροφής της πληροφορίας και των αγαθών στο τέλος, ή σε προκαθορισμένο σημείο της συμφωνία, την εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα καθώς και κάθε άλλη σχετική ιδιότητα των αγαθών, τους περιορισμούς σχετικά με την αντιγραφή και αποκάλυψη πληροφορίας.
   γ) Εκπαίδευση χρηστών και διαχειριστών σε μεθόδους, διαδικασίες και ασφάλεια.
   δ) Διασφάλιση επίγνωσης από τους χρηστές των ευθυνών τους σε θέματα ασφάλειας.
   ε) Πρόβλεψη μεταφοράς προσωπικού, όποτε κρίνεται απαραίτητο.
   ς) Καθήκοντα σχετικά με την εγκατάσταση και συντήρηση του υλικού και του λογισμικού.
   ζ) Μία καθαρή δομή και προσυμφωνημένα πρότυπα αναφορών.
   η) Πολιτική ελέγχου πρόσβασης.
   θ) Καθορισμός επαληθεύσιμων κριτηρίων απόδοσης.
   ι) Η δυνατότητα ελέγχου των αρμοδιοτήτων που καθορίζονται στη συμφωνία, από τρίτους, απαριθμώντας τα νόμιμα δικαιώματα των ελεγκτών.
   ια) Η καθιέρωση μιας διαδικασίας κλιμάκωσης στην επίλυση των προβλημάτων.
   ιβ) Απαιτήσεις συνέχειας των υπηρεσιών, συμπεριλαμβανομένων και μέτρων για την διαθεσιμότητα και αξιοπιστία, σύμφωνα πάντα με τις προτεραιότητες του οργανισμού.
   ιγ) Συμμετοχή τρίτων μέσω υπεργολάβων, και οι έλεγχοι ασφαλείας που οι τελευταίοι πρέπει να εφαρμόσουν.

ιδ) Όροι επαναδιαπραγμάτευσης και επανακαθορισμού της συμφωνίας σε περίπτωση αλλαγής των απαιτήσεων ασφαλείας.
ιε) Σχέδιο έκτακτης ανάγκης σε περίπτωση που κάποιο μέρος θέλει να υπαναχωρήσει.
ις) Καταγραφή των αγαθών, αδειών εκμετάλλευσης, συμβολαίων ή δικαιωμάτων που σχετίζονται με αυτά.

2.5 Διαχείριση Αγαθών

2.5.1 Επιμερισμός ευθυνών

Τα αγαθά του οργανισμού πρέπει να προστατεύονται επαρκώς και με τα κατάλληλα μέτρα ασφαλείας. Όλα τα αγαθά πρέπει να καταμετρηθούν και να έχουν ένα ορισμένο 'ιδιοκτήτη', ο οποίος θα είναι υπεύθυνος και για την τήρηση ελέγχου τους. Η εφαρμογή ελέγχων ρουτίνας δύναται να ανατεθεί σε άλλον από τον 'ιδιοκτήτη', αλλά σε κάθε περίπτωση η ευθύνη για την προστασία των αγαθών παραμένει σε αυτόν.

1. <u>*Κατάλογος με τα αγαθά:*</u> Θα πρέπει να γίνει απογραφή όλων των αγαθών του οργανισμού, να καταρτισθεί και να τηρείται κατάλογος αυτών. Στον κατάλογο αυτό πρέπει να αναφέρεται η σπουδαιότητα κάθε αγαθού και να περιέχεται κάθε απαραίτητη πληροφορία για την ανάκτησή του σε περίπτωση καταστροφής. Βάσει της σπουδαιότητας του αγαθού, της επιχειρησιακής του αξίας και της διαβάθμισης ασφαλείας του, θα πρέπει να προσδιορίζονται τα επίπεδα προστασίας. Υπάρχουν πολλών ειδών αγαθά:
    α) Πληροφορία: βάσεις δεδομένων, αρχεία δεδομένων, συμβόλαια και συμφωνίες, τεκμηρίωση συστήματος, έρευνες, εγχειρίδια χρηστών, εκπαιδευτικό υλικό, λειτουργικές και διαδικασίες υποστήριξης, σχέδια συνέχειας επιχειρησιακής δραστηριότητας, ρυθμίσεις υπαναχώρησης, λογιστικοί έλεγχοι, αρχειοθετημένη πληροφορία.
    β) Λογισμικό εφαρμογών, συστήματος, εργαλεία ανάπτυξης και βοηθήματα.
    γ) Φυσικά αγαθά: υπολογιστικός και τηλεπικοινωνιακός εξοπλισμός, αφαιρούμενα μέσα.
    δ) Υπηρεσίες πληροφορικής και επικοινωνιών, γενικές υπηρεσίες όπως θέρμανση, ψύξη, φωτισμός, ενέργεια.
    ε) Το ανθρώπινο προσωπικό και τα προσόντα, δεξιότητες και εμπειρία τους.
    ς) Άυλα αγαθά, όπως η φήμη και εικόνα του οργανισμού.
2. <u>*'Ιδιοκτησία' αγαθών:*</u> Κάθε πληροφορία και αγαθό που σχετίζεται με τα ΠΣ θα πρέπει να ανήκει σε ορισμένο τμήμα του οργανισμού, το οποίο θα είναι υπεύθυνο: α) για τη σωστή ταξινόμησή τους και β) για τον ορισμό και περιοδική αναθεώρηση της ταξινόμησης αυτής και των περιορισμών πρόσβασης βάσει της ισχύουσας πολιτικής ελέγχου πρόσβασης. Στην περίπτωση πολύπλοκων ΠΣ, που είναι δυνατή η ύπαρξη ομάδων αγαθών, που ενεργούν μαζί για την παροχή μίας συγκεκριμένης λειτουργίας-υπηρεσίας, η ευθύνη παροχής της υπηρεσίας καθώς και της λειτουργίας των αγαθών, ανήκει στον 'ιδιοκτήτη' της υπηρεσίας.
3. <u>*Αποδεκτή χρήση αγαθών:*</u> Κάθε υπάλληλος, εργολάβος, τρίτος χρήστης θα πρέπει να ακολουθεί συγκεκριμένους κανόνες για την αποδεκτή χρήση των αγαθών των ΠΣ, όπως, κανόνες για το ηλεκτρονικό ταχυδρομείο και τη χρήση του Διαδικτύου, καθώς και οδηγίες για τη χρήση φορητών συσκευών, ειδικά όσον αφορά τη χρήση τους εκτός των εγκαταστάσεων του οργανισμού.

2.5.2 Διαβάθμιση πληροφορίας

Οι πληροφορίες που διαχειρίζεται ο οργανισμός θα πρέπει να διαβαθμίζονται ανάλογα με τις ανάγκες, προτεραιότητες και τον αναμενόμενο βαθμό ασφαλείας, καθώς έχουν διαφορετικό βαθμό ευαισθησίας και κρισιμότητας. Ορισμένα στοιχεία μπορεί να απαιτούν πρόσθετα επίπεδα προστασίας ή ιδιαίτερη μεταχείριση, για τον καθορισμό των οποίων ίσως είναι απαραίτητο ένα σχήμα διαβάθμισης της πληροφορίας.

1. <u>*Οδηγίες διαβάθμισης:*</u> Η διαβάθμιση της πληροφορίας πρέπει να γίνει βάσει της αξίας της, το βαθμό ευαισθησίας της, την κρισιμότητά της για τον οργανισμό και τις νομικές απαιτήσεις που

διέπουν την επεξεργασία της. Η διαβάθμιση και οι σχετιζόμενοι έλεγχοι προστασίας της πληροφορίας πρέπει να βασίζονται στις επιχειρησιακές ανάγκες για ανταλλαγή ή περιορισμό της πληροφορίας και επιπτώσεις που σχετίζονται με αυτές. Οι οδηγίες πρέπει να περιλαμβάνουν συμβάσεις για την αρχική διαβάθμιση καθώς και την τακτική αναθεώρησή αυτής, σύμφωνα με κάποια προκαθορισμένη πολιτική ελέγχου πρόσβασης. Είναι ευθύνη του 'ιδιοκτήτη' του κάθε αγαθού να ορίζει το βαθμό διαβάθμισής του και να το επαναξιολογεί τακτικά, για να διασφαλίζει ότι είναι ενημερωμένο και στο κατάλληλο επίπεδο. Θα πρέπει να εξετασθεί ο αριθμός των διαβαθμίσεων και τα οφέλη από τη χρήση τους. Υπερβολικά πολύπλοκα σχήματα, μπορεί να είναι αντιοικονομικά και ανέφικτα.

2. *Κατηγοριοποίηση και χειρισμός πληροφορίας:* Πρέπει να αναπτυχθεί και να υλοποιηθεί ένα κατάλληλο σχήμα για την κατηγοριοποίηση και τη διαχείριση των πληροφοριών. Οι διαδικασίες κατηγοριοποίησης πρέπει να καλύπτουν αγαθά είτε φυσικής είτε ηλεκτρονικής μορφής. Η έξοδος των ΠΣ που περιέχει πληροφορία χαρακτηρισμένη ευαίσθητη ή κρίσιμη θα πρέπει να κατηγοριοποιηθεί. Τέτοια στοιχεία εξόδου για παράδειγμα, είναι οι αναφορές, οθόνες υπολογιστών, συσκευές εγγραφής, ηλεκτρονικά μηνύματα και μεταφορές αρχείων.

2.6 Ασφάλεια προσωπικού

2.6.1 Πριν την πρόσληψη

Το προσωπικό, οι υπεργολάβοι και οι χρήστες τρίτων μερών πρέπει να κατανοούν τις ευθύνες τους, και να διαθέτουν τα κατάλληλα προσόντα για τους ρόλους που αναλαμβάνουν, ώστε να μειωθεί ο κίνδυνος κλοπής, απάτης ή κακής χρήσης των εγκαταστάσεων. Οι αρμοδιότητες και οι ρόλοι ασφαλείας, καθώς και οι προϋποθέσεις απασχόλησης, πρέπει να προσδιορίζονται πριν την πρόσληψη και να είναι καταγεγραμμένες στις περιγραφές των θέσεων εργασίας. Όλοι οι υποψήφιοι για πρόσληψη, ειδικά για ευαίσθητες θέσεις εργασίας, πρέπει να έχουν ελεγχθεί καταλλήλως. Τέλος, το προσωπικό, οι υπεργολάβοι και τρίτοι χρήστες των ΠΣ, πρέπει να υπογράψουν συμφωνητικό για τους ρόλους και τις αρμοδιότητες τους που σχετίζονται με την ασφάλεια των ΠΣ του οργανισμού.

1. *Ρόλοι και αρμοδιότητες:* οι ρόλοι και αρμοδιότητες του προσωπικού και των υπεργολάβων πρέπει να ορίζονται και τεκμηριώνονται σύμφωνα με την πολιτική ασφαλείας του οργανισμού. Ο ορισμός των ρόλων πρέπει να διασφαλίζει ότι δε θα γίνεται επικάλυψη αρμοδιοτήτων του προσωπικού και ότι θα καλύπτονται οι αρμοδιότητες που αφορούν τη διαχείριση της ασφάλειας των ΠΣ.
2. *Έλεγχος:* απαιτείται έλεγχος ασφαλείας (έλεγχος των συστάσεων, ταυτότητας, των πιστοποιητικών σπουδών κλπ), για όλο το καινούριο προσωπικό, σύμφωνα με τη νομοθεσία. Στην περίπτωση που μία θέση εργασίας, είτε πρόκειται για νέα πρόσληψη, είτε για προαγωγή, επιτρέπει στον εργαζόμενο να έχει πρόσβαση στα ΠΣ του οργανισμού και ιδίως όταν χειρίζεται ευαίσθητη πληροφορία (π.χ. οικονομικά θέματα) ο έλεγχος θα πρέπει να είναι πιο λεπτομερής.
3. *Όροι και συνθήκες πρόσληψης:* μέρος των υποχρεώσεων του εργαζομένου που απορρέουν από τη σύμβαση εργασίας είναι και οι αρμοδιότητές του σχετικά με την ασφάλεια των ΠΣ. Οι όροι και οι συνθήκες πρόσληψης πρέπει να βασίζονται στην πολιτική ασφαλείας του οργανισμού και οι εργαζόμενοι θα πρέπει να δεσμεύονται με συμβόλαιο εμπιστευτικότητας ή μη αποκάλυψης προτού τους δοθεί πρόσβαση στα ΠΣ του οργανισμού, το οποίο σε ορισμένες περιπτώσεις θα ισχύει για καθορισμένο χρόνο ακόμα και μετά τη λήξη της σύμβασης εργασίας.

2.6.2 Κατά τη διάρκεια της απασχόλησης

Πρέπει να διασφαλισθεί ότι το προσωπικό και οι υπεργολάβοι κατανοούν τις απειλές και τα ζητήματα ασφαλείας, τις ευθύνες και υποχρεώσεις τους και ότι είναι σε θέση να εφαρμόσουν την πολιτική ασφαλείας κατά την εργασία τους, ώστε να ελαττώσουν τον κίνδυνο ανθρώπινου λάθους (ακούσιου ή εσκεμμένου). Πρέπει να καθορισθούν συγκεκριμένες αρμοδιότητες διαχείρισης για να διασφαλισθεί ότι η εργασία κάθε υπαλλήλου μέσα στον οργανισμό γίνεται υπό τους όρους ασφαλείας. Κάθε εργαζόμενος, υπεργολάβος ή χρήστης από τρίτα μέρη πρέπει να είναι κατάλληλα εκπαιδευμένος,

καταρτισμένος, αλλά και συνειδητοποιημένος, όσον αφορά τις διαδικασίες ασφαλείας και σωστής χρήσης των ΠΣ, ώστε να ελαχιστοποιηθούν οι κίνδυνοι, ενώ θα πρέπει να καθιερωθεί μία επίσημη πειθαρχική διαδικασία για το χειρισμό παραβιάσεων ασφαλείας.

1. *Αρμοδιότητες διαχείρισης:* το προσωπικό, οι υπεργολάβοι και τρίτοι χρήστες πρέπει να είναι σωστά ενημερωμένοι για τους ρόλους και τα καθήκοντά τους πριν τους δοθεί η πρόσβαση σε ευαίσθητη πληροφορία ή στα ΠΣ του οργανισμού. Θα πρέπει να καθοδηγούνται κατάλληλα, να τους δίνονται κίνητρα για την εκπλήρωση των πολιτικών ασφαλείας του οργανισμού, αλλά και να εξακολουθούν να κατέχουν τα απαραίτητα προσόντα και δεξιότητες για την εκάστοτε θέση που αναλαμβάνουν.
2. *Εκπαίδευση κατάρτιση και ευαισθητοποίηση σε θέματα Ασφαλείας:* Πρέπει να παρέχεται επαρκής, κατάλληλη και συνεχής εκπαίδευση στο προσωπικό, ανάλογα με το ρόλο που ο κάθε εργαζόμενος ή συνεργάτης έχει στη λειτουργία των ΠΣ του οργανισμού. Η συνεχής εκπαίδευση πρέπει να περιλαμβάνει απαιτήσεις ασφαλείας, νομικές υποχρεώσεις, να είναι προς την κατεύθυνση στης σωστής χρήσης των ΠΣ (π.χ. διαδικασίες εισόδου χρήστη, χρήση πακέτων λογισμικού, κλπ) και να είναι ανάλογη με το ρόλο, τα καθήκοντα και τις δυνατότητες του κάθε εργαζομένου.
3. *Διαδικασία πειθαρχικού ελέγχου:* πρέπει να υπάρχει μία επίσημη διαδικασία πειθαρχικού ελέγχου για τους εργαζομένους που διέπραξαν παραβίαση ασφαλείας, και η οποία θα διασφαλίζει μία δίκαιη αντιμετώπιση για αυτούς που είναι ύποπτοι για την παραπάνω ενέργεια. Μέσα από την παραπάνω διαδικασία θα πρέπει να λαμβάνονται υπόψη η φύση και η βαρύτητα της παραβίασης καθώς και ο αντίκτυπος που είχε στον οργανισμό, εάν είναι η πρώτη φορά ή πρόκειται για υπότροπο, εάν ήταν εκπαιδευμένος, η σχετική νομοθεσία καθώς και κάθε άλλος παράγοντας που απαιτείται. Σε σοβαρά περιστατικά θα πρέπει να είναι άμεση η απομάκρυνση από τα καθήκοντά του, άρση των δικαιωμάτων πρόσβασης, ακόμα και άμεση συνοδεία εκτός της περιοχής του περιστατικού.

2.6.3 Καταγγελία ή τροποποίηση της σύμβασης εργασίας

Η καταγγελία ή τροποποίηση μίας σύμβασης εργασίας με έναν εργαζόμενο ή μίας συμφωνίας με έναν υπεργολάβο θα πρέπει να γίνει με ομαλό τρόπο και θα πρέπει να διασφαλισθεί η επιστροφή όλου του εξοπλισμού και η αφαίρεση όλων των δικαιωμάτων πρόσβασης που μπορεί να είχαν παραχωρηθεί σε αυτό τον εργαζόμενο ή υπεργολάβο.

1. *Ενέργειες κατά την απόλυση:* το τμήμα Ανθρώπινου Δυναμικού είναι υπεύθυνο για τη διαδικασία της καταγγελίας της σύμβασης, και σε συνεργασία με το διευθυντή του απολυόμενου διαχειρίζεται τα θέματα ασφαλείας που προκύπτουν.
2. *Επιστροφή των αγαθών:* Κάθε εργαζόμενος ή συνεργάτης πρέπει να επιστρέφει κάθε αγαθό (π.χ. λογισμικό, εταιρικά έγγραφα και εξοπλισμό, κινητές υπολογιστικές συσκευές, κάρτες εισόδου, εγχειρίδια, πληροφορία αποθηκευμένη σε ηλεκτρονικά μέσα, κλπ) που ανήκει στον οργανισμό και έχει περιέλθει στην κατοχή του λόγω της σχέσης εργασίας που είχε συνάψει και η οποία έληξε. Στις περιπτώσεις που ο εργαζόμενος ή συνεργάτης αγοράζει τον εξοπλισμό του οργανισμού ή ακόμα που χρησιμοποιεί δικό του προσωπικό εξοπλισμό πρέπει να ακολουθούνται διαδικασίες ώστε κάθε σχετική πληροφορία να μεταφέρεται στον οργανισμό και να διαγράφεται από τον εξοπλισμό. Τέλος, όταν δεν πρόκειται για εξοπλισμό, αλλά για γνώση η οποία όμως είναι σημαντική, τότε αυτή πρέπει να τεκμηριώνεται και να μεταφέρεται μέσα στον οργανισμό.
3. *Άρση των δικαιωμάτων πρόσβασης:* Με την καταγγελία ή τροποποίηση της σύμβασης πρέπει να αφαιρούνται και τα δικαιώματα πρόσβασης στην πληροφορία και στα ΠΣ του οργανισμού. Τα δικαιώματα πρόσβασης περιλαμβάνουν τόσο τη φυσική και όσο και τη λογική πρόσβαση, κλειδιά, κάρτες ταυτοποίησης, συνδρομές, αλλά και απομάκρυνσή τους από κάθε έγγραφο που τον αναγνωρίζει ως εν ενεργεία μέλος του οργανισμού. Εάν ο εργαζόμενος ή συνεργάτης με τον οποίο διακόπτεται η σύμβαση ή συμφωνία γνωρίζει κωδικούς πρόσβασης σε ενεργούς λογαριασμούς τότε αυτοί θα πρέπει να αλλάξουν. Σε ορισμένες περιπτώσεις μάλιστα, τα δικαιώματα πρόσβασης θα πρέπει να μειωθούν ή αφαιρεθούν τελείως πριν ακόμα την καταγγελία της σύμβασης ή συμφωνίας, ανάλογα με την εκτίμηση της επικινδυνότητας, ώστε να αποφευχθεί εσκεμμένη παραποίηση πληροφορίας και δολιοφθορά των ΠΣ του οργανισμού.. Στην περίπτωση, που το

άτομο που απολύεται ανήκει σε μία ομάδα χρηστών με συγκεκριμένα δικαιώματα, τότε θα διαγράφεται από αυτή την ομάδα και θα γίνονται συστάσεις στα υπόλοιπα μέλη να μη μοιράζονται πλέον πληροφορία με αυτόν.

2.7 Φυσική και περιβαλλοντολογική ασφάλεια

2.7.1 Ασφάλεια χώρων

Η κρίσιμη και ευαίσθητη πληροφορία και τα ΠΣ του οργανισμού πρέπει να στεγάζονται σε ασφαλείς χώρους και να προστατεύονται, με στόχο την αποτροπή μη εξουσιοδοτημένης φυσικής πρόσβασης σε αυτά, που θα μπορούσε να προκαλέσει την φθορά ή ακόμα και την καταστροφή τους. Η προστασία αυτή θα πρέπει να ανάλογη της επικινδυνότητας.

1. <u>*Ασφάλεια περιμέτρου:*</u> πρέπει να ορισθεί σαφής περίμετρος του κτιρίου ή του χώρου όπου είναι εγκατεστημένα τα ΠΣ του οργανισμού, με ιδιαίτερη προσοχή ώστε να μην προκύπτουν κενά ασφαλείας. Οι εξωτερικοί τοίχοι πρέπει να είναι στιβαρής κατασκευής και όλες οι εξωτερικές πόρτες να διαθέτουν μηχανισμούς ελέγχου πρόσβασης (επανδρωμένοι χώροι υποδοχής, μπάρες, συναγερμοί, κλειδαριές, συστήματα εντοπισμού εισβολέα κλπ). Τα ΠΣ του οργανισμού δε θα πρέπει να είναι εγκατεστημένα στον ίδιο χώρο με αυτά που διαχειρίζονται από τρίτους, ενώ ιδιαίτερη προσοχή, όσον αφορά τον έλεγχο πρόσβασης, θα πρέπει να δοθεί στις περιπτώσεις όπου στο ίδιο κτίριο στεγάζονται παραπάνω από ένας οργανισμοί.
2. <u>*Έλεγχος εισόδου:*</u> Η είσοδος στους χώρους όπου είναι εγκατεστημένα τα ΠΣ του οργανισμού θα πρέπει να είναι πλήρως ελεγχόμενη και θα πρέπει να τηρείται αρχείο καταγραφής με την ώρα και την ημερομηνία της εισόδου και της αποχώρησης επισκεπτών, η παρουσία των οποίων θα επιβλέπεται και θα τους χορηγείται άδεια για συγκεκριμένο σκοπό.
3. <u>*Ασφάλεια γραφείων, δωματίων και εγκαταστάσεων:*</u> Πρέπει να σχεδιασθούν και εφαρμοσθούν μέτρα προστασίας της φυσικής ασφάλειας των γραφείων, δωματίων και εγκαταστάσεων όπου βρίσκονται τα ΠΣ του οργανισμού, λαμβάνοντας υπόψη τις σχετικές διατάξεις και πρότυπα υγείας και ασφάλειας. Οι εγκαταστάσεις ‘κλειδιά’ θα πρέπει να είναι τοποθετημένες σε σημείο όπου να αποτρέπεται η πρόσβαση από το κοινό, αποφεύγοντας χρησιμοποίηση έντονων ενδείξεων, μέσα ή έξω από το κτίριο, που θα δηλώνουν την ύπαρξη τους.
4. <u>*Προστασία ενάντια σε εξωτερικές και περιβαλλοντολογικές απειλές:*</u> Πρέπει να σχεδιασθούν και εφαρμοσθούν μέτρα προστασίας από πυρκαϊά, πλημμύρα, σεισμό, έκρηξη, αναταραχή και κάθε άλλη μορφή φυσικής ή ανθρώπινης απειλής, ενώ θα πρέπει να ληφθούν υπόψη τυχόν απειλές που θα παρουσιασθούν από γειτονικά κτίρια, όπως μία πυρκαϊά σε ένα γειτονικό κτίριο, μία διαρροή από την ταράτσα ή το υπόγειο, μία έκρηξη στο δρόμο. Τα επικίνδυνα ή εύφλεκτα υλικά θα πρέπει να αποθηκεύονται σε μία ασφαλή απόσταση από την εγκατάσταση, ενώ μαζικές προμήθειες, όπως η γραφική ύλη, θα πρέπει να αποθηκεύονται σε ξεχωριστό χώρο. Ο εφεδρικός εξοπλισμός και τα αντίγραφα ασφαλείας, θα πρέπει να κρατούνται σε ασφαλή απόσταση, ώστε μία καταστροφή που θα πλήξει την κύρια εγκατάσταση να μην τα επηρεάσει. Τέλος, πρέπει να υπάρχει πυροσβεστικός εξοπλισμός και να είναι κατάλληλα τοποθετημένος.
5. <u>*Εργασία στους χώρους ασφαλείας:*</u> Το προσωπικό θα γνωρίζει την ύπαρξη ή τις δραστηριότητες σε ένα χώρο ασφαλείας μόνο εάν απαιτείται από τα καθήκοντά του, και θα πρέπει να υπάρχουν συγκεκριμένες οδηγίες για την εργασία μέσα στους χώρους αυτούς. Οι χώροι οι οποίοι είναι κενοί θα πρέπει να κλειδώνονται και ελέγχονται τακτικά.
6. <u>*Δημόσια πρόσβαση, παράδοση και χώροι φόρτωσης:*</u> σημεία πρόσβασης, όπως χώροι παράδοσης και φόρτωσης, από όπου μπορούν να εισέλθουν άτομα χωρίς εξουσιοδότηση, θα πρέπει να ελέγχονται και όσο είναι δυνατό να είναι απομονωμένα από τις εγκαταστάσεις ΠΣ του οργανισμού. Οι εξωτερικές πόρτες των χώρων παράδοσης και φόρτωσης, θα πρέπει να είναι ασφαλισμένες όταν οι εσωτερικές πόρτες είναι ανοιχτές. Το εισερχόμενο υλικό πρέπει να επιθεωρηθεί για πιθανές απειλές πριν μεταφερθεί στις εσωτερικές εγκαταστάσεις, καθώς και να καταχωρηθεί σύμφωνα με τις διαδικασίες διαχείρισης αγαθών. Οι εισερχόμενες αποστολές θα πρέπει να είναι διαχωρισμένες από τις εξερχόμενες όσο αυτό είναι δυνατό.

2.7.2 Ασφάλεια εξοπλισμού

Για την αποφυγή απώλειας, καταστροφής, κλοπής ή διακινδύνευσης των αγαθών και κατ' επέκταση διακοπή των δραστηριοτήτων του οργανισμού ο εξοπλισμός θα πρέπει να προστατεύεται από φυσικές και περιβαλλοντολογικές απειλές. Για το σκοπό αυτό πρέπει να εξετασθεί η διάθεση και τοποθέτηση του εξοπλισμού, αλλά και έλεγχος βοηθητικών εγκαταστάσεων, όπως η παροχή ηλεκτρικού ρεύματος και η υποδομή καλωδίωσης.

1. *Τοποθέτηση και προστασία εξοπλισμού:* ο εξοπλισμός πρέπει να είναι τοποθετημένος και προστατευμένος ώστε να μειώνεται ο κίνδυνος από φυσικές και περιβαλλοντολογικές απειλές. Η κατανάλωση φαγητού, ποτού και το κάπνισμα μέσα στις εγκαταστάσεις ΠΣ απαγορεύονται. Οι κλιματολογικές συνθήκες στους χώρους, όπως θερμοκρασία και υγρασία, που μπορούν να επηρεάσουν τη λειτουργία των ΠΣ, πρέπει να παρακολουθούνται.
2. *Υποστηρικτικοί μηχανισμοί:* ο εξοπλισμός θα πρέπει να προστατεύεται από αστοχίες ή βλάβες υποστηρικτικών μηχανισμών, όπως ηλεκτρική παροχή, παροχή νερού, αποχέτευση, θέρμανση, εξαερισμός, κλιματισμός, οι οποίοι θα πρέπει να ελέγχονται για τη σωστή λειτουργία τους. Η παροχή ηλεκτρικού ρεύματος θα πρέπει να είναι κατάλληλη με τις απαιτήσεις του κατασκευαστή. Συστήνεται η λειτουργία συσκευής αδιάλειπτης παροχής ρεύματος (UPS) για την ομαλή διακοπή λειτουργίας ειδικά του εξοπλισμό που υποστηρίζει βασικές λειτουργίες του οργανισμού, καθώς και σχέδιο έκτακτης ανάγκης σε περίπτωση που αυτή αποτύχει. Για περιπτώσεις παρατεταμένης παροχής ρεύματος, συστήνεται η ύπαρξη εφεδρικής γεννήτριας, με διαθέσιμη ικανή ποσότητα καυσίμου για να διασφαλισθεί η λειτουργία της κατά τη διάρκεια της διακοπής. Οι συσκευές αυτές και οι γεννήτριες θα πρέπει να ελέγχονται και δοκιμάζονται για τη σωστή λειτουργία τους. Οι διακόπτες ηλεκτρικού ρεύματος θα πρέπει να βρίσκονται κοντά στις εξόδους των εγκαταστάσεων για την άμεση διακοπή λειτουργίας σε περίπτωση ανάγκης. Οι εγκαταστάσεις θα πρέπει να είναι εξοπλισμένες φωτισμό έκτακτης ανάγκης σε περίπτωση αστοχίας της κύριας πηγής ενέργειας. Η παροχή νερού πρέπει να είναι σταθερή και κατάλληλη για την τροφοδοσία του κλιματισμού, του εξοπλισμού ύγρανσης και του συστήματος πυρκαγιάς. Ο τηλεπικοινωνιακός εξοπλισμός, πρέπει να συνδέεται με τον πάροχο, τουλάχιστον με δύο διαφορετικές γραμμές για την αποφυγή αποτυχίας σύνδεσης, ενώ οι υπηρεσίες φωνής πρέπει να επαρκούν για την ικανοποίηση επικοινωνιών έκτακτης ανάγκης. Προτείνεται η εγκατάσταση συστήματος ειδοποίησης σε περίπτωση που παρουσιασθούν δυσλειτουργίες στους παραπάνω μηχανισμούς.
3. *Ασφάλεια καλωδίωσης:* οι γραμμές ηλεκτροδότησης και τηλεπικοινωνιών πρέπει να προστατεύονται από δολιοφθορές και υποκλοπές, γι' αυτό το λόγο αν είναι δυνατό θα πρέπει να είναι υπόγειες. Η χρήση κοινών καλωδίων ή διαδρομών μέσα από κοινόχρηστους χώρους πρέπει να αποφεύγεται στη δικτυακή καλωδίωση. Τα καλώδια ρεύματος θα πρέπει να διαχωρίζονται από αυτά των επικοινωνιών. Για τα κρίσιμα ΠΣ απαιτούνται περαιτέρω μέτρα προστασίας, όπως εγκατάσταση θωρακισμένων αγωγών, κλειδωμένων δωματίων στα τερματικά σημεία, χρήση εναλλακτικών διαδρομών και μέσων μετάδοσης, χρήση καλωδίων οπτικών ινών, τεχνικές σάρωσης και φυσικών επιθεωρήσεων για τον εντοπισμό μη εξουσιοδοτημένων συσκευών που να έχουν συνδεθεί στα καλώδια και ελεγχόμενη πρόσβαση στα δωμάτια και πίνακες καλωδίωσης (patch panels).
4. *Συντήρηση εξοπλισμού:* για τη διατήρηση της διαθεσιμότητας και σωστής λειτουργίας του εξοπλισμού αυτός πρέπει να συντηρείται σύμφωνα με τις υποδείξεις και προδιαγραφές του κατασκευαστή και στα συνιστώμενα χρονικά διαστήματα. Η συντήρηση και οι επιδιορθώσεις πρέπει να γίνονται μόνο από εξουσιοδοτημένο προσωπικό, καθώς και να τηρείται αρχείο τις βλάβες και τις προληπτικές και διορθωτικές ενέργειες. Όταν η συντήρηση γίνεται από εξωτερικούς συνεργάτες, κάθε ευαίσθητη πληροφορία που περιέχεται στον εξοπλισμό πρέπει να διαγράφεται.
5. *Ασφάλεια εξοπλισμού εκτός της εγκατάστασης:* ανεξάρτητα της ιδιοκτησίας, η χρήση εξοπλισμού επεξεργασίας πληροφορίας του οργανισμού έξω από τις εγκαταστάσεις πρέπει να γίνεται με άδεια από τη διοίκηση. Οι κίνδυνοι (φθορά, κλοπή ή υποκλοπή) μπορεί να διαφέρουν σε σημαντικό βαθμό ανάλογα με την τοποθεσία, κάτι που πρέπει να ληφθεί υπόψη για τον καθορισμό κατάλληλων ελέγχων.

6. <u>Ασφαλής απόρριψη ή επαναχρησιμοποίηση του εξοπλισμού:</u> ο εξοπλισμός που περιέχει συσκευές αποθήκευσης πρέπει να ελεγχθεί ότι τυχόν ευαίσθητη πληροφορία ή αδειοδοτημένο λογισμικό έχει διαγραφεί ή επανεγγραφεί με ασφάλεια προτού σταλεί για απόρριψη. Συσκευές που περιέχουν ευαίσθητη πληροφορία πρέπει να καταστρέφονται ή θα πρέπει η πληροφορία αυτή να καταστρέφεται, διαγράφεται ή επανεγγράφεται χρησιμοποιώντας τεχνικές που θα την κάνουν μη προσπελάσιμη και όχι χρησιμοποιώντας τη τυποποιημένη διαδικασία διαγραφής ή μορφοποίησης.
7. <u>Απομάκρυνση εξοπλισμού:</u> απαγορεύεται η απομάκρυνση του εξοπλισμού εκτός του οργανισμού χωρίς εξουσιοδότηση. Η απομάκρυνση του εξοπλισμού πρέπει να έχει συγκεκριμένα χρονικά όρια και να γίνεται έλεγχος της επιστροφής εντός αυτών. Όπου είναι απαραίτητο πρέπει να γίνεται καταγραφή απομάκρυνσης και επιστροφής του εξοπλισμού. Εξουσιοδοτημένο προσωπικό μπορεί να προβαίνει σε επιτόπιους δειγματοληπτικούς ελέγχους για τον εντοπισμό μη εξουσιοδοτημένης απομάκρυνσης του εξοπλισμού.

2.8 Διαχείριση επικοινωνιών και λειτουργιών

2.8.1 Λειτουργικές διαδικασίες και αρμοδιότητες

Πρέπει να υπάρχουν συγκεκριμένες αρμοδιότητες και διαδικασίες όσον αφορά τη διαχείριση των ΠΣ του οργανισμού, με στόχο τη διασφάλιση της σωστής και ασφαλούς λειτουργίας τους. Επίσης, όπου είναι απαραίτητο, με σωστό διαχωρισμό καθηκόντων μπορεί να επιτευχθεί μείωση της κατάχρησης των ΠΣ του οργανισμού είτε αυτά είναι εσκεμμένη είτε από αμέλεια.

1. <u>Τεκμηρίωση των διαδικασιών λειτουργίας:</u> οι διαδικασίες λειτουργίας των ΠΣ του οργανισμού πρέπει να είναι τεκμηριωμένες, να τηρούνται και να είναι διαθέσιμες σε κάθε χρήστη. Πρέπει να δίνονται σαφείς οδηγίες σχετικά με την επεξεργασία και χειρισμό της πληροφορίας, τη δημιουργία αντιγράφων ασφαλείας, τον προγραμματισμό των εργασιών, την αντιμετώπιση σφαλμάτων που μπορεί να εμφανισθούν κατά την εκτέλεση μίας εργασίας, συμπεριλαμβανομένων περιορισμών αναφορικά με τη χρήση υποστηρικτικών προγραμμάτων, τηλέφωνα επικοινωνίας όταν παρουσιασθούν λειτουργικές και τεχνικές δυσκολίες, διαδικασίες επανεκκίνησης ή επαναφοράς των συστημάτων σε περίπτωση βλάβης, τη διαχείριση του συστήματος καταγραφής πληροφοριών.
2. <u>Διαχείριση αλλαγών:</u> πρέπει να υπάρχει έλεγχος για τις όποιες αλλαγές γίνονται στα ΠΣ του οργανισμού. Ειδικά, τα λειτουργικά συστήματα και το λογισμικό εφαρμογών πρέπει να υπόκεινται σε αυστηρό έλεγχο διαχείρισης αλλαγών. Πρέπει να γίνεται καταγραφή, σχεδιασμός, δοκιμή και σχετική έγκριση για κάθε αλλαγή. Επίσης, πρέπει να υπάρχουν εναλλακτικές διαδικασίες για ματαίωση ή ανάκτηση από αποτυχημένες αλλαγές ή απρόβλεπτες καταστάσεις. Οι αλλαγές στα λειτουργικά συστήματα πρέπει να γίνονται μόνο όταν υπάρχει σημαντικός επιχειρησιακός λόγος, π.χ. για μείωση κινδύνου του συστήματος. Η αναβάθμιση των συστημάτων με νεότερες εκδόσεις μπορεί να εισάγουν περισσότερες αλλαγές και αστάθεια σε σχέση με την τρέχουσα έκδοση.
3. <u>Διαχωρισμός καθηκόντων:</u> είναι μία μέθοδος για τη μείωση του κινδύνου από ατυχηματική ή εσκεμμένη κατάχρηση των συστημάτων του οργανισμού.
4. <u>Διαχωρισμός λειτουργικών εργασιών, ανάπτυξης και δοκιμών:</u> πρέπει να προσδιορισθούν τα επίπεδα διαχωρισμού του περιβάλλοντος ανάπτυξης, δοκιμών και λειτουργίας για την αποφυγή προβλημάτων. Θα πρέπει να τεθούν κανόνες για τη μεταφορά του λογισμικού από την ανάπτυξη στην λειτουργική κατάσταση. Τα λογισμικά ανάπτυξης και λειτουργίας θα πρέπει να τρέχουν σε διαφορετικά συστήματα και σε διαφορετικά πεδία (domains)ή καταλόγους, διότι οι ενέργειες ανάπτυξης και δοκιμών μπορούν να προκαλέσουν σοβαρά προβλήματα π.χ. βλάβη συστήματος, με επιθυμητή τροποποίηση δεδομένων. Οι μεταγλωττιστές και τα άλλα εργαλεία ανάπτυξης και βοηθητικά προγράμματα δεν πρέπει να είναι προσβάσιμα από τα λειτουργικά συστήματα (όταν δεν απαιτείται). Το περιβάλλον του συστήματος δοκιμών θα πρέπει να προσομοιάζει όσο το δυνατό πιο πιστά το περιβάλλον λειτουργίας.

2.8.2 Διαχείριση υπηρεσιών από τρίτους

Οι υπηρεσίες που παρέχονται από τρίτους πρέπει να διασφαλίζουν το κατάλληλο επίπεδο ασφαλείας, σύμφωνα με τα όσα προβλέπει η πολιτική ασφαλείας του οργανισμού και σε συνδυασμό με την τήρηση των συμβατικών υποχρεώσεων σχετικά με την ποιότητα των παρεχόμενων υπηρεσιών.

1. *Παράδοση υπηρεσίας:* ο οργανισμός πρέπει να διασφαλίζει ότι τηρούνται τα μέτρα ασφαλείας, οι προδιαγραφές της παρεχόμενης υπηρεσίας και το επίπεδο αυτής, όπως αναγράφονται στη σχετική συμφωνία.
2. *Παρακολούθηση και αξιολόγηση της παρεχόμενης υπηρεσίας:* Οι υπηρεσίες που παρέχονται από τρίτους πρέπει να παρακολουθούνται και αξιολογούνται τακτικά, για τη διασφάλιση τήρησης των όρων και προϋποθέσεων ασφαλείας. Η ευθύνη της διαχείρισης των σχέσεων με τον πάροχο της υπηρεσίας πρέπει να ανατίθεται σε ένα εξουσιοδοτημένο άτομο ή σε μία ομάδα διαχείρισης της υπηρεσίας.
3. *Διαχείριση αλλαγών σε υπηρεσίες τρίτων:* οι αλλαγές σε υπηρεσίες από τρίτους, συμπεριλαμβανομένων των υφιστάμενων πολιτικών, διαδικασιών και ελέγχων ασφαλείας, πρέπει να διαχειρίζονται, λαμβάνοντας υπόψη την κρισιμότητα των συστημάτων και διαδικασιών του οργανισμού που εμπλέκονται και επανεκτιμώντας τους κινδύνους. Πρέπει να γίνει ε΄νας διαχωρισμός μεταξύ των αλλαγών που εφαρμόζονται από τον οργανισμό και αλλαγών που εφαρμόζονται σε υπηρεσίες τρίτων.

2.8.3 Προγραμματισμός και αποδοχή συστήματος

Απαιτείται έγκαιρος προγραμματισμός και προετοιμασία για την εξασφάλιση της απαιτούμενης διαθεσιμότητας σε χωρητικότητα και πόρους με στόχο την απαιτούμενη απόδοση των συστημάτων. Επίσης, θα πρέπει να γίνουν προβλέψεις των μελλοντικών αναγκών σε χωρητικότητα, για τη μείωση του κινδύνου υπερφόρτωσης των συστημάτων, ενώ θα πρέπει να καθορισθούν, τεκμηριωθούν και εξετασθούν οι λειτουργικές απαιτήσεις νέων συστημάτων πριν την έγκρισή τους και χρήση τους.

1. *Διαχείριση χωρητικότητας:* η χρήση των πόρων πρέπει να παρακολουθείται και να συντονίζεται, και παράλληλα να προβλέπονται οι μελλοντικές ανάγκες για την εξασφάλιση της αποδοτικότητας των ΠΣ του οργανισμού. Πρέπει να εντοπίζονται οι απαιτήσεις χωρητικότητας για κάθε νέα και τρέχουσα δραστηριότητα, ενώ ιδιαίτερη προσοχή πρέπει να δοθεί στους πόρους για τους οποίους απαιτείται μεγάλη ανάγκη σε προμήθεια ή έχουν υψηλό κόστος. Οι διαχειριστές πρέπει να προλαμβάνουν ενδεχόμενη συμφόρηση και να αποφεύγουν την εξάρτηση από στελέχη που θα μπορούσαν να αποτελέσουν απειλή για την ασφάλεια των ΠΣ και των υπηρεσιών, λαμβάνοντας κατάλληλα μέτρα.
2. *Αποδοχή συστημάτων:* πρέπει να πληρούνται συγκεκριμένα κριτήρια για την αποδοχή νέων ΠΣ, αναβαθμίσεων ή εκδόσεων και να διεξάγονται κατάλληλες δοκιμές του/ων συστημάτων κατά την ανάπτυξή τους και πριν την παραλαβή τους. Σε όλα τα στάδια της ανάπτυξης θα πρέπει να ζητείται η γνώμη των χρηστών για να διασφαλισθεί η λειτουργική αποδοτικότητα του προτεινόμενου σχεδίου συστήματος.

2.8.4 Προστασία από κακόβουλο ή απομακρυσμένο λογισμικό

Τα ΠΣ και το λογισμικό του οργανισμού είναι ευάλωτα σε επιθέσεις κακόβουλου λογισμικού όπως ιοί υπολογιστών, σκουλήκια, δούρειους ίππους, κλπ. Είναι αναγκαία η λήψη προφυλάξεων για τον εντοπισμό και αποτροπή εισόδου κακόβουλου και μη εξουσιοδοτημένου απομακρυσμένου λογισμικού με στόχο την προστασία της ακεραιότητας του λογισμικού και της πληροφορίας.

1. *Έλεγχοι από κακόβουλο λογισμικό:* η προστασία από κακόβουλο λογισμικού θα πρέπει να βασίζεται σε μέτρα ανίχνευσης, πρόληψης και ανάκαμψης από αντίστοιχες επιθέσεις, αλλά και στην κατάλληλη εκπαίδευση και ενημέρωση των χρηστών. Επομένως, απαραίτητη είναι η εγκατάσταση και τακτική ενημέρωση λογισμικού εντοπισμού και επιδιόρθωσης, και η σάρωση των υπολογιστών και των ηλεκτρονικών μέσων ως μία διαδικασία ρουτίνας. Για βελτίωση της αποτελεσματικότητας συστήνεται η χρήση δύο ή περισσοτέρων προϊόντων λογισμικού

προστασίας από κακόβουλο κώδικα, και εάν αυτό είναι δυνατό από διαφορετικούς προμηθευτές. Πρέπει να γίνεται έλεγχος των συνημμένων αρχείων των ηλεκτρονικών μηνυμάτων, των ληφθέντων αρχείων, αλλά και των ιστοσελίδων για τον εντοπισμό κακόβουλου λογισμικού. Οι διαχειριστές ασφαλείας θα πρέπει να είναι ενημερωμένοι συλλέγοντας κάθε σχετική πληροφορία είτε μέσα από εγγραφή σε λίστες ηλεκτρονικού ταχυδρομείου, σε έγκριτα περιοδικά ή αξιόπιστες ιστοσελίδες, και να διακρίνουν τις πραγματικές απειλές από τις φάρσες.

2. *Έλεγχοι από απομακρυσμένο λογισμικό:* το απομακρυσμένο λογισμικό είναι τμήμα κώδικα που μεταφέρεται από τον έναν υπολογιστή σε έναν άλλο και εκτελεί αυτόματα κάποια συγκεκριμένη διεργασία με ελάχιστη ή και καθόλου διεπαφή με το χρήστη. Το απομακρυσμένο λογισμικό μπορεί να σχετίζεται με μια σειρά ενδιάμεσων υπηρεσιών (middleware services). Μέτρα προστασίας από απομακρυσμένο λογισμικό είναι η εκτέλεσή του σε απομονωμένο περιβάλλον, η αποτροπή χρήσης ή παραλαβής τέτοιου λογισμικού, η εφαρμογή κρυπτογραφημένων ελέγχων για την αυθεντικοποίηση του κώδικα αυτού.

2.8.5 Αντίγραφα ασφαλείας

Πρέπει να υπάρχουν διαδικασίες ρουτίνας για την εφαρμογή της πολιτικής και στρατηγικής για τη δημιουργία αντιγράφων ασφαλείας, με στόχο τη διατήρηση της ακεραιότητας και διαθεσιμότητας της πληροφορίας και των ΠΣ του οργανισμού.

1. *Δημιουργία αντιγράφων ασφαλείας:* θα πρέπει να λαμβάνονται και ελέγχονται τακτικά αντίγραφα ασφαλείας της πληροφορίας και του λογισμικού σύμφωνα με τα όσα ορίζει η πολιτική αντιγράφων ασφαλείας, ώστε να εξασφαλίζεται ότι η ευαίσθητη πληροφορία και το λογισμικό μπορούν να ανακτηθούν ύστερα από καταστροφή ή βλάβη του συστήματος. Οπότε, θα πρέπει να καθορισθούν ακριβείς και ολοκληρωμένες εγγραφές αντιγράφων ασφαλείας και τεκμηριωμένες διαδικασίες ανάκτησης, το εύρος και η συχνότητά τους τα οποία θα πρέπει να καλύπτουν τις απαιτήσεις ασφαλείας του οργανισμού, τα αντίγραφα ασφαλείας πρέπει να αποθηκεύονται σε ξεχωριστό χώρο και να ελέγχονται τακτικά για την αξιοπιστία τους, και τέλος, στις περιπτώσεις που είναι σημαντική η εμπιστευτικότητα, τα αντίγραφα ασφαλείας πρέπει να προστατεύονται από μέσα κρυπτογράφησης. Για κρίσιμα συστήματα, η διαδικασία λήψης αντιγράφων ασφαλείας, πρέπει να καλύπτει όλα τα δεδομένα, εφαρμογές και πληροφορία που είναι απαραίτητη για την ανάκτηση όλου του συστήματος μετά από καταστροφή.

2.8.6 Διαχείριση δικτυακής ασφάλειας

Πρέπει να διασφαλίζεται η προστασία της δικτυακής πληροφορίας, καθώς και οι υποστηρικτικές δικτυακές εγκαταστάσεις. Η διαχείριση ασφαλείας των δικτύων, η οποία μπορεί να καλύπτει τα όρια του οργανισμού, απαιτεί προσεκτική εξέταση της ροής δεδομένων, των νομικών προεκτάσεων, της παρακολούθησης και προστασίας. Πρόσθετοι έλεγχοι απαιτούνται για την προστασία της ευαίσθητης πληροφορίας που περνά μέσα από δημόσια δίκτυα.

1. *Μέσα δικτυακής ασφάλειας:* τα δίκτυα πρέπει να διαχειρίζονται και ελέγχονται κατάλληλα, για να προστατεύονται από απειλές και να διατηρούν την ασφάλεια των συστημάτων και εφαρμογών που τα χρησιμοποιούν, συμπεριλαμβανομένης της μεταφερόμενης πληροφορίας. Ειδικοί έλεγχοι απαιτούνται για τη διαφύλαξη της εμπιστευτικότητας και ακεραιότητας των δεδομένων που μεταφέρονται στα δημόσια και ασύρματα δίκτυα και για την προστασία των συνδεδεμένων συστημάτων και εφαρμογών, αλλά και τη διατήρηση της διαθεσιμότητας των δικτυακών υπηρεσιών και των συνδεδεμένων υπολογιστών.
2. *Ασφάλεια των δικτυακών υπηρεσιών:* σε κάθε συμφωνητικό παροχής δικτυακών υπηρεσιών (είτε αυτές παρέχονται από τρίτους είτε όχι) πρέπει να περιλαμβάνονται τα χαρακτηριστικά ασφαλείας, το επίπεδο της παρεχόμενης υπηρεσίας και οι απαιτήσεις διαχείρισης. Παράλληλα θα πρέπει να παρακολουθείται η ικανότητα του πάροχου να διαχειρίζεται τις συμφωνημένες υπηρεσίες με ασφαλή τρόπο. Οι δικτυακές υπηρεσίες περιλαμβάνουν την παροχή των συνδέσεων, υπηρεσίες ιδιωτικών δικτύων, δίκτυα προστιθέμενης αξίας και λύσεις διαχείρισης δικτυακής ασφάλειας, όπως τείχη προστασίας (firewalls) και συστήματα εντοπισμού εισβολέα.

2.8.7 Διαχείριση μέσων αποθήκευσης

Είναι απαραίτητος ο έλεγχος και η φυσική προστασία των μέσων αποθήκευσης, με στόχο την αποτροπή αποκάλυψης, τροποποίησης, αφαίρεσης ή καταστροφής των αγαθών χωρίς εξουσιοδότηση, και κατ' επέκταση της διακοπής των δραστηριοτήτων του οργανισμού. Γι' αυτό το λόγο είναι απαραίτητη η εφαρμογή διαδικασιών για την προστασία των εγγράφων, μέσων αποθήκευσης, δεδομένων εισόδου/εξόδου και τεκμηρίωσης των συστημάτων.

1. *Διαχείριση αφαιρούμενων μέσων:* πρέπει να υπάρχουν διαδικασίες για τη διαχείριση των αφαιρούμενων μέσων αποθήκευσης, όπως κασέτες, δισκέτες, εξωτερικοί σκληροί δίσκοι, CDs, DVDs, USBs κλπ. Τα περιεχόμενα κάθε επαναχρησιμοποιήσιμου μέσου που πρόκειται να απομακρυνθεί από τον οργανισμό πρέπει να γίνουν μη ανακτήσιμα, ενώ θα πρέπει να τηρείται και σχετικό αρχείο με τις απομακρύνσεις. Πληροφορία που αποθηκεύεται σε μέσο και πρέπει να κρατηθεί περισσότερο από το εκτιμώμενο χρόνο ζωής της συσκευής από τον κατασκευαστή της, θα πρέπει να αποθηκεύεται και αλλού για αποφυγή απώλειας της πληροφορίας λόγω παλαιότητας του μέσου.
2. *Καταστροφή των μέσων:* τα μέσα αποθήκευσης πρέπει να καταστρέφονται με ασφαλή τρόπο, όταν δεν απαιτείται άλλο η χρήση τους, ακολουθώντας αυστηρώς καθορισμένες διαδικασίες, με στόχο την μείωση του κινδύνου διαρροής ευαίσθητης πληροφορίας σε μη εξουσιοδοτημένα άτομα.
3. *Διαδικασίες χειρισμού πληροφοριών:* πρέπει να ορισθούν διαδικασίες για το χειρισμό, επεξεργασία, αποθήκευση και διαβίβαση της πληροφορίας ανάλογα με την κατηγοριοποίησή της. Θα πρέπει να σημανθούν τα μέσα αποθήκευσης κατάλληλα ανάλογα με το επίπεδο κατηγοριοποίησης τους, να καθορισθούν περιορισμοί πρόσβασης σε αυτά και να τηρείται επίσημο αρχείο των εξουσιοδοτημένων αποδεκτών των δεδομένων.
4. *Ασφάλεια αρχείων τεκμηρίωσης:* τα αρχεία τεκμηρίωσης μπορούν να περιέχουν περιγραφές των εφαρμογών, των διεργασιών και διαδικασιών, της δομής των δεδομένων και των εξουσιοδοτημένων προσβάσεων. Γι' αυτό το λόγο πρέπει να αποθηκεύονται με ασφάλεια και η πρόσβαση σε αυτά να είναι περιορισμένη και να ελέγχεται από τον 'ιδιοκτήτη' της κάθε εφαρμογής.

2.8.8 Ανταλλαγή πληροφοριών

Η ανταλλαγή πληροφοριών και λογισμικού μεταξύ οργανισμών πρέπει να βασίζεται σε μία επίσημη πολιτική ανταλλαγής, και η οποία θα πρέπει να συμμορφώνεται με τη σχετική νομοθεσία. Θα πρέπει να καθορισθούν διαδικασίες και πρότυπα για την προστασία της πληροφορίας και του λογισμικού που ανταλλάσσονται εντός και εκτός του οργανισμού.

1. *Πολιτικές και διαδικασίες ανταλλαγής πληροφορίας:* πρέπει να υπάρχουν διαδικασίες για την προστασία της ανταλλασσόμενης πληροφορίας από υποκλοπή, αντιγραφή, τροποποίηση, εσφαλμένη δρομολόγηση, καταστροφή, μεταφορά κακόβουλου λογισμικού ή μεταφορά ευαίσθητης πληροφορίας που περιέχεται στα συνημμένα αρχεία. Επίσης, πρέπει να υπάρχουν μία συγκεκριμένη πολιτική ή οδηγίες που θα περιγράφουν την ορθή χρήση των ηλεκτρονικών και ασύρματων μέσων επικοινωνίας. Συστήνεται η χρήση τεχνικών κρυπτογράφησης για τη διατήρηση της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας της πληροφορίας. Γενικότερα, η πληροφορία θα μπορούσε τεθεί σε κίνδυνο λόγω έλλειψης ενημέρωσης, πολιτικής ή διαδικασιών, π.χ. κάποιος να κρυφακούσει ένα τηλεφώνημα που έγινε σε δημόσιο χώρο ή ένα αυτόματο τηλεφωνητή, λόγω μίας εσφαλμένης αποστολής ενός ηλεκτρονικού ή τηλεομοιοτυπικού μηνύματος κλπ. Γι' αυτό το λόγο, θα πρέπει να υπενθυμίζεται στο προσωπικό κατά την εκτέλεση της εργασίας του να μην αφήνει ευαίσθητη ή κρίσιμη πληροφορία στα φωτοαντιγραφικά μηχανήματα, στους εκτυπωτές και στις συσκευές τηλεομοιοτυπίας, καθώς και να τους εφιστάται η προσοχή στο ότι τα νέας τεχνολογίας μηχανήματα διαθέτουν κρυφές μνήμες και σε περίπτωση σφάλματος μετάδοσης ή χαρτιού, τυπώνουν το έγγραφο μόλις το σφάλμα αποκατασταθεί, αλλά και να αποφεύγουν να συζητούν ευαίσθητα θέματα του οργανισμού σε μη ασφαλείς χώρους.
2. *Κανόνες ανταλλαγής δεδομένων/πληροφοριών:* πρέπει να τεθούν συγκεκριμένοι κανόνες για την ανταλλαγή πληροφοριών και λογισμικού εντός και εκτός του οργανισμού, όπως διοικητικές

αρμοδιότητες για τον έλεγχο, κοινοποίηση, μετάδοση, αποστολή και παραλαβή τους, διαδικασίες ειδοποίησης του αποστολέα για την μετάδοση, αποστολή και παραλαβή, αλλά και για τη διασφάλιση της ιχνηλασιμότητας και μη άρνησης της ευθύνης.

3. *Μεταφορά φυσικών μέσων αποθήκευσης:* θα πρέπει να λαμβάνονται μέτρα προστασίας απέναντι στη μη εξουσιοδοτημένη πρόσβαση, κακή χρήση ή διαφθορά της πληροφορίας που περιέχεται σε μέσα αποθήκευσης κατά τη μεταφορά τους εκτός των φυσικών ορίων του οργανισμού. Πρέπει να υπάρχει εγκεκριμένη λίστα από τη διοίκηση με τους εξουσιοδοτημένους μεταφορείς οι οποίοι θα πρέπει να είναι έμπιστοι. Επίσης, θα πρέπει να υπάρχουν διαδικασίες εξακρίβωσης της ταυτότητας των μεταφορέων. Η συσκευασία θα πρέπει να είναι κατάλληλη ώστε να προστατεύει το περιεχόμενο από οποιαδήποτε φυσική ζημιά που μπορεί να προκύψει κατά τη μεταφορά, για παράδειγμα προστασία απέναντι σε περιβαλλοντικούς παράγοντες που μπορεί να μειώσουν την αποτελεσματικότητα ανάκτησης των μέσων, όπως η έκθεση σε θερμότητα, υγρασία ή ηλεκτρομαγνητικά πεδία.
4. *Ανταλλαγή ηλεκτρονικών μηνυμάτων:* τα μηνύματα ηλεκτρονικού ταχυδρομείου, η ηλεκτρονική ανταλλαγή δεδομένων (Electronic Data Interchange-EDI) και η ανταλλαγή άμεσων μηνυμάτων παίζουν σημαντικό ρόλο στην επικοινωνία του οργανισμού και αντιμετωπίζουν διαφορετικούς κινδύνους από τις κλασσικές επικοινωνίες, καθώς μπορούν να περιέχουν ευαίσθητη πληροφορία. Γι' αυτό το λόγο πρέπει να ληφθούν μέτρα ασφαλείας, όπως, προστασία των μηνυμάτων από μη εξουσιοδοτημένη πρόσβαση, τροποποίηση ή άρνηση της υπηρεσίας, διασφάλιση ότι το μήνυμα αποστέλλεται στη σωστή διεύθυνση, γενικότερη αξιοπιστία και διαθεσιμότητα της υπηρεσίας, απαιτήσεις για τη χρήση ψηφιακών υπογραφών, λήψη έγκρισης πριν τη χρησιμοποίηση εξωτερικών δημόσιων υπηρεσιών, όπως υπηρεσίες άμεσων μηνυμάτων ή διαμοιρασμός αρχείων (file sharing).
5. *Επιχειρηματικά πληροφοριακά συστήματα:* τα ΠΣ γραφείου δίνουν τη δυνατότητα ταχύτερης διάδοσης και διαμοιρασμού της επιχειρηματικής πληροφορίας συνδυάζοντας έγγραφα, Η/Υ, κινητές επικοινωνίες, ηλεκτρονικό ταχυδρομείο, ψηφιακούς τηλεφωνητές, πολυμέσα, τηλεομοιοτυπικές συσκευές και ταχυδρομείο. Επομένως, θα πρέπει να αναπτυχθούν πολιτικές και διαδικασίες για την προστασία της πληροφορίας που συνδέεται με τη ενδοεπικοινωνία των επιχειρηματικών ΠΣ, οι οποίες θα περιλαμβάνουν τρωτότητες των διοικητικών και λογιστικών συστημάτων, όπου η πληροφορία διαμοιράζεται μεταξύ των διαφόρων τμημάτων του οργανισμού, τρωτότητες στα συστήματα επικοινωνίας του οργανισμού, όπως καταγραφή τηλεφωνικών κλήσεων, απόρρητο κλήσεων, αποθήκευση των τηλεομοιοτυπικών εγγράφων, άνοιγμα μηνυμάτων ηλεκτρονικού ταχυδρομείου, διανομή αλληλογραφίας, περιορισμό επιλεγμένων συστημάτων σε συγκεκριμένες κατηγορίες χρηστών και τοποθεσίες από όπου μπορεί να γίνει η πρόσβαση.

2.8.9 Υπηρεσίες ηλεκτρονικού εμπορίου

Πρέπει να διασφαλίζεται η προστασία και η ασφαλής χρήση των υπηρεσιών ηλεκτρονικού εμπορίου. Γι' αυτό το λόγο πρέπει να εξετάζονται οι συνέπειες που έχει η χρήση αυτών των υπηρεσιών, συμπεριλαμβανομένων των διαδικτυακών συναλλαγών, αλλά και η διατήρηση της ακεραιότητας και διαθεσιμότητας της πληροφορίας που μεταδίδεται ηλεκτρονικά και διαμέσου δημόσια διαθέσιμων συστημάτων.

1. *Ηλεκτρονικό εμπόριο:* οι πληροφορίες που σχετίζονται με το ηλεκτρονικό εμπόριο και διακινούνται μέσω δημοσίων δικτύων πρέπει να προστατεύονται από απάτη, μη εξουσιοδοτημένη αποκάλυψη και τροποποίηση, αλλά και διενέξεις που αφορούν συμβόλαια και συμβάσεις. Θα πρέπει να εξετασθούν το επίπεδο της αμοιβαίας εμπιστοσύνης σχετικά με την ταυτότητα των συμβαλλομένων μερών και οι διαδικασίες εξουσιοδότησης που σχετίζονται με το ποιος μπορεί να καθορίζει τις τιμές, να εκδίδει ή υπογράφει έγγραφα-κλειδιά των συναλλαγών. Επίσης, πρέπει να καθορισθούν και να πληρούνται οι προϋποθέσεις για εμπιστευτικότητα, ακεραιότητα, απόδειξη παράδοσης και παραλαβής εγγράφων, και μη καταγγελίας των συμβολαίων, ο βαθμός εξακρίβωσης των στοιχείων πληρωμής που παρέχονται από τον πελάτη και άλλες ασφαλιστικές απαιτήσεις. Τέλος, πρέπει να ληφθούν μέτρα προστασίας για τη διατήρηση της εμπιστευτικότητας

και ακεραιότητας των πληροφοριών παραγγελίας, την αποφυγή απώλειας ή επικάλυψης συναλλαγών και τις αστικές ευθύνες που προκύπτουν από παράνομες συναλλαγές.

2. *Διαδικτυακές συναλλαγές:* οι πληροφορίες που αφορούν συναλλαγές στο διαδίκτυο πρέπει να προστατεύονται από ελλιπή μετάδοση, λανθασμένη δρομολόγηση, αλλοίωση, μη εξουσιοδοτημένη αποκάλυψη και επαναμετάδοση μηνύματος. Τα θέματα ασφαλείας που ανακύπτουν με τις διαδικτυακές συναλλαγές πρέπει να περιλαμβάνουν τη χρήση ηλεκτρονικών υπογραφών για το κάθε συμβαλλόμενο μέρος που μετέχει στη συναλλαγή, τα αναγνωριστικά χρήστη κάθε μέρους είναι έγκυρα και επαληθευμένα, ασφαλή πρωτόκολλα και μονοπάτια επικοινωνίας μεταξύ των μερών, αποθήκευση των δεδομένων των συναλλαγών σε τοποθεσία που δεν είναι άμεσα προσβάσιμη από το διαδίκτυο, π.χ. το εσωτερικό δίκτυο (intranet) του οργανισμού. Οι συναλλαγές μπορεί να υπόκεινται σε διαφορετικούς νόμους, κανόνες και κανονισμούς ανάλογα με τη δικαιοδοσία της περιοχής όπου γίνεται η έναρξη, η επεξεργασία, η ολοκλήρωση και αποθήκευση της συναλλαγής.
3. *Δημόσια διαθέσιμη πληροφορία:* η ακεραιότητα των πληροφοριών που βρίσκονται σε δημόσια διαθέσιμα ΠΣ πρέπει να προστατεύεται, ώστε να αποτρέπεται η μη εξουσιοδοτημένη τροποποίησή τους. Τα δημόσια διαθέσιμα ΠΣ πρέπει να δοκιμάζονται για εντοπισμό αδυναμιών και αποτυχιών προτού δημοσιοποιηθεί σε αυτά η πληροφορία. Τα ηλεκτρονικά συστήματα δημοσίευσης και ειδικά εκείνα που επιτρέπουν την άμεση είσοδο και ανατροφοδότηση πληροφορίας πρέπει να ελέγχονται προσεκτικά, ώστε να συμμορφώνονται με τη σχετική νομοθεσία για την προστασία των δεδομένων. Η πρόσβαση σε ένα σύστημα δημοσίευσης δε θα επιτρέπει την ταυτόχρονη πρόσβαση και στα δίκτυα με τα οποία είναι συνδεδεμένο.

2.8.10 Παρακολούθηση

Τα ΠΣ του οργανισμού πρέπει να παρακολουθούνται και να γίνεται καταγραφή των περιστατικών ασφαλείας, με στόχο τον εντοπισμό μη εξουσιοδοτημένων ενεργειών. Τα αρχεία καταγραφής λειτουργίας και σφαλμάτων μπορούν να χρησιμοποιηθούν για την εξασφάλιση του εντοπισμού των προβλημάτων ασφαλείας των ΠΣ. Οι διαδικασίες παρακολούθησης και καταγραφής του οργανισμού πρέπει να συμμορφώνονται με όλες τις σχετικές νομικές απαιτήσεις. Το σύστημα παρακολούθησης μπορεί να χρησιμοποιηθεί για τη διαπίστωση της αποτελεσματικότητας των διενεργούμενων ελέγχων και την εξακρίβωση της συμμόρφωσης με ένα μοντέλο πολιτικής πρόσβασης.

1. *Τήρηση αρχείων καταγραφής δεδομένων:* πρέπει να λαμβάνονται αρχεία καταγραφής (log files) και να τηρούνται για ένα συμφωνημένο χρονικό διάστημα ώστε να αξιοποιηθούν για τη διενέργεια ελέγχου. Τα αρχεία καταγραφής πρέπει να περιλαμβάνουν αναγνωριστικά χρηστών, ημερομηνίες και ώρες σύνδεσης και αποσύνδεσης, ταυτότητα ή τοποθεσία τερματικού, αρχείο επιτυχημένων και μη προσπαθειών σύνδεσης, αλλαγές στη διαμόρφωση του συστήματος, δικαιώματα χρηστών, χρήση εφαρμογών και βοηθητικών προγραμμάτων, αρχεία που προσπελάσθηκαν και με ποιον τρόπο, διευθύνσεις και πρωτόκολλα δικτύου, ενεργοποίηση και απενεργοποίηση λογισμικού προστασίας από κακόβουλο λογισμικό ή συστημάτων εντοπισμού εισβολέα, κλπ. Τέλος, εάν είναι δυνατό, οι διαχειριστές των ΠΣ να μην έχουν δικαίωμα διαγραφής ή απενεργοποίησης των αρχείων καταγραφής της δικής τους δραστηριότητας.
2. *Χρήση συστήματος παρακολούθησης:* πρέπει να υπάρχουν διαδικασίες για την παρακολούθηση της χρήσης των ΠΣ του οργανισμού. Τα αποτελέσματα του συστήματος παρακολούθησης πρέπει να ελέγχονται σε τακτική βάση. Το επίπεδο παρακολούθησης των ΠΣ καθορίζεται από μία ανάλυση επικινδυνότητας και καλύπτει τομείς όπως αναγνωριστικά χρηστών, ημερομηνία και ώρα πρόσβασης, αρχεία που προσπελάσθηκαν, προγράμματα που χρησιμοποιηθήκαν, χρήση λογαριασμών διαχειριστή, εκκίνηση και διακοπή λειτουργίας συστήματος, σύνδεση και αποσύνδεση συσκευών, αποτυχημένες ενέργειες χρηστών, ειδοποιήσεις τείχους προστασίας και δικτυακών πυλών, συναγερμοί συστήματος, εξαιρέσεις αρχείων καταγραφής συστήματος, αλλαγές ή απόπειρα αλλαγών των ρυθμίσεων του συστήματος. Η συχνότητα που αξιολογούνται τα αποτελέσματα της παρακολούθησης εξαρτάται από παράγοντες επικινδυνότητας όπως, η κρισιμότητα της εφαρμογής, η αξία, η ευαισθησία και η κρισιμότητα της πληροφορίας, τυχόν

πρότερη εμπειρία αναφορικά με κατάχρηση και διείσδυση στο σύστημα, και απενεργοποίηση των αρχείων καταγραφής δεδομένων.

3. *Προστασία των δεδομένων καταγραφής:* τα συστήματα και τα δεδομένα καταγραφής πρέπει να προστατεύονται από μη εξουσιοδοτημένη πρόσβαση ή αλλοίωση. Ιδιαίτερη προσοχή πρέπει να δοθεί σε τυχόν μεταβολή του τύπου των μηνυμάτων που καταγράφονται, στην επεξεργασία ή διαγραφή των αρχείων καταγραφής, και στη χωρητικότητα των μέσων αποθήκευσης αρχείων καταγραφής, που εάν γεμίσει μπορεί να έχει ως αποτέλεσμα την αποτυχία καταγραφής συμβάντων ή επανεγγραφή παλιότερα καταγεγραμμένων συμβάντων. Τα αρχεία καταγραφής περιέχουν ένα μεγάλο όγκο πληροφορίας η οποία μπορεί να είναι άσχετη με την παρακολούθηση της ασφάλειας του ΠΣ. Για τον εντοπισμό των σημαντικών γεγονότων συστήνεται η αυτόματη αντιγραφή των κατάλληλων τύπων μηνυμάτων σε ένα δεύτερο αρχείο, από όπου χρησιμοποιώντας κατάλληλα βοηθητικά προγράμματα ή εργαλεία ελέγχου γίνεται ανάλυση της πληροφορίας.
4. *Αρχεία καταγραφής διαχειριστή και χειριστή:* οι ενέργειες των διαχειριστών και χειριστών συστημάτων πρέπει να καταγράφονται και να αξιολογούνται σε τακτική βάση.
5. *Καταγραφή λαθών και αστοχιών:* Οι αστοχίες των συστημάτων πρέπει να καταγράφονται, αναλύονται, και να πραγματοποιούνται οι κατάλληλες ενέργειες για την αντιμετώπισή τους, καθώς μπορεί να έχουν σοβαρό αντίκτυπο στην απόδοση των συστημάτων.
6. *Συγχρονισμός ρολογιών συστήματος:* τα ρολόγια των ΠΣ του οργανισμού πρέπει να είναι συγχρονισμένα. Καθώς ένας υπολογιστής ή μία συσκευή επικοινωνίας έχει τη δυνατότητα να λειτουργήσει σε πραγματικό χρόνο, το ρολόι της συσκευής θα πρέπει να ορισθεί σύμφωνα με κάποιο πρότυπο για παράδειγμα ώρα UTCή στην τοπική ώρα. Επίσης, πρέπει να υπάρχει μία διαδικασία ελέγχου και διόρθωσης του ρολογιού όταν παρατηρείται μεγάλη διακύμανση. Μπορεί να χρησιμοποιηθεί ένα πρωτόκολλο δικτυακής ώρας το οποίο να κρατάει συγχρονισμένους όλους τους εξυπηρετητές με ένα κύριο ρολόι που θα έχει ορισθεί.

2.9 Έλεγχος πρόσβασης

2.9.1 Επιχειρησιακές απαιτήσεις για έλεγχο πρόσβασης

Η πρόσβαση στην πληροφορία, τα ΠΣ και τις επιχειρηματικές διαδικασίες του οργανισμού πρέπει να ελέγχεται σύμφωνα με τις επιχειρησιακές και απαιτήσεις ασφαλείας. Επίσης, οι κανόνες για τον έλεγχο πρόσβασης πρέπει να συμμορφώνονται με τις πολιτικές διάδοσης και εξουσιοδότησης της πληροφορίας.

1. *Πολιτική ελέγχου πρόσβασης:* οι κανόνες και τα δικαιώματα πρόσβασης για κάθε χρήστη ή ομάδα χρηστών θα πρέπει να δηλώνονται με σαφήνεια σε μία πολιτική ελέγχου πρόσβασης. Η πολιτική αυτή θα πρέπει να περιλαμβάνει: α) απαιτήσεις ασφαλείας για κάθε εφαρμογή του οργανισμού, β*)* προσδιορισμό όλης της πληροφορία που σχετίζεται με τις εφαρμογές και των κινδύνων που αυτή αντιμετωπίζει, γ) συνοχή μεταξύ του ελέγχου πρόσβασης και των πολιτικών κατηγοριοποίησης της πληροφορίας μεταξύ διαφορετικών συστημάτων και δικτύων, δ) σχετική νομοθεσία και υποχρεώσεις που απορρέουν από σχετικές συμβάσεις, ε) τυποποιημένα προφίλ χρηστών για τις πιο κοινές εργασίες στον οργανισμό, στ) διαχείριση των δικαιωμάτων πρόσβασης σε κατανεμημένα και δικτυακά περιβάλλοντα, ζ) διαχωρισμό των ρόλων ελέγχου πρόσβασης (αίτημα πρόσβασης, άδεια πρόσβασης, διαχείριση), η) απαιτήσεις για την επίσημη έγκριση επί των αιτήσεων πρόσβασης, θ) περιοδική επανεξέταση των ελέγχων πρόσβασης και ι) αφαίρεση δικαιωμάτων πρόσβασης. Κατά τη θέσπιση των κανόνων πρόσβασης, πρέπει να υπάρχει μια διαφοροποίηση μεταξύ των κανόνων που ισχύουν πάντα και των υπολοίπων οδηγιών οι οποίες είναι προαιρετικές ή εκτελούνται υπό προϋποθέσεις. Επίσης, το σκεπτικό των κανόνων πρέπει να βασίζεται στην υπόθεση ότι *«όλα γενικά απαγορεύονται εκτός εάν ρητά επιτρέπονται»* παρά στην πιο αδύναμη *«όλα γενικά επιτρέπονται εκτός εάν ρητά απαγορεύονται»*.

2.9.2 Διαχείριση πρόσβασης

Πρέπει να υπάρχουν επίσημες διαδικασίες ελέγχου της διάθεσης δικαιωμάτων πρόσβασης στα ΠΣ και υπηρεσίες του οργανισμού. Οι διαδικασίες πρέπει να καλύπτουν όλα τα στάδια του κύκλου ζωής, από την αρχική εγγραφή νέων χρηστών μέχρι την τελική διαγραφή τους από τη στιγμή που δεν απαιτείται άλλο η πρόσβασή τους στα ΠΣ του οργανισμού και τις υπηρεσίες. Ιδιαίτερη προσοχή πρέπει να δοθεί στην ανάγκη για έλεγχο της διάθεσης προνομιακών δικαιωμάτων, τα οποία επιτρέπουν στους χρήστες να παρακάμπτουν τους ελέγχους συστήματος.

1. <u>*Εγγραφή χρήστη:*</u> πρέπει να υπάρχει μία τυπική διαδικασία για την εγγραφή και διαγραφή ενός χρήστη για τη χορήγηση και ανάκληση αντίστοιχα πρόσβασής του στα ΠΣ του οργανισμού και τις υπηρεσίες. Η διαδικασία αυτή θα πρέπει να περιλαμβάνει: α) τη χρήση μοναδικών αναγνωριστικών χρηστών που να τους συνδέει και καθιστά υπεύθυνους για τις ενέργειές τους (η χρήση ομάδων αναγνωριστικών θα επιτρέπεται μόνο για επιχειρησιακούς και λειτουργικούς λόγους), β) έλεγχο ότι ο χρήστης έχει την άδεια του 'ιδιοκτήτη' για τη χρήση του ΠΣ ή υπηρεσίας, γ) γραπτή δήλωση των δικαιωμάτων πρόσβασης, δ) υπογεγραμμένη δήλωση των χρηστών ότι κατανοούν τους όρους πρόσβασης, ε)διασφάλιση ότι οι πάροχοι υπηρεσιών δεν επιτρέπουν την πρόσβαση προτού ολοκληρωθούν οι διαδικασίες εξουσιοδότησης, στ)τήρηση επίσημου αρχείου όλων των εγγεγραμμένων ατόμων που χρησιμοποιούν κάθε υπηρεσία, ζ)τακτικός έλεγχος και άμεση αφαίρεση ή αποκλεισμό των δικαιωμάτων πρόσβασης στους χρήστες που έχουν αλλάξει καθήκοντα, θέση εργασίας ή έφυγαν από τον οργανισμό.
2. <u>*Διαχείριση δικαιωμάτων πρόσβασης:*</u> η χορήγηση δικαιωμάτων πρόσβασης πρέπει να είναι περιορισμένη και να ελέγχεται αυστηρά μέσα από μία τυπική διαδικασία. Θα πρέπει να εντοπισθούν και καταγραφούν τα δικαιώματα πρόσβασης σε κάθε επιμέρους σύστημα (π.χ. λειτουργικό σύστημα, σύστημα διαχείρισης βάσεων δεδομένων , εφαρμογές κλπ) και οι χρήστες στους οποίους εκχωρούνται. Συστήνεται η ανάπτυξη και η χρήση ρουτινών συστήματος και προγραμμάτων για την αποφυγή ανάγκης εκτέλεσης με δικαιώματα.
3. <u>*Διαχείριση συνθηματικών:*</u> αρχικά πρέπει να παρέχεται στους χρήστες ένα ασφαλές προσωρινό συνθηματικό, το οποίο υποχρεούνται να το αλλάξουν αμέσως. Πριν την παροχή ενός νέου, προσωρινού ή αντικατάστασης συνθηματικού πρέπει να γίνεται επαλήθευση της ταυτότητας του χρήστη. Η χορήγηση προσωρινών κωδικών πρέπει να γίνεται με ασφαλή τρόπο (π.χ. αποφυγή αποστολής μέσω ηλεκτρονικού ταχυδρομείου). Τα συνθηματικά δεν πρέπει να αποθηκεύονται στους υπολογιστές, ενώ προεπιλεγμένοι κωδικοί πρόσβασης θα πρέπει να τροποποιούνται μετά την εγκατάσταση του συστήματος ή του λογισμικού.
4. <u>*Αναθεώρηση δικαιωμάτων πρόσβασης:*</u> τα δικαιώματα πρόσβασης πρέπει να αναθεωρούνται ανά τακτά διαστήματα (π.χ. κάθε εξάμηνο) ή μετά από αλλαγές (π.χ. προαγωγή, υποβιβασμό ή λήξη της απασχόλησης), ενώ οι αναθεωρήσεις για τα ιδιαίτερα προνομιακά δικαιώματα θα πρέπει να είναι πιο συχνές (π.χ. κάθε τρίμηνο).

2.9.3 Ευθύνες χρηστών

Η συμπεριφορά των χρηστών για την αποφυγή μη εξουσιοδοτημένης πρόσβασης και αλλοίωσης ή ακόμα και κλοπής πληροφορίας ή συστημάτων είναι ουσιώδης. Οι χρήστες πρέπει να έχουν επίγνωση των ευθυνών τους για τέλεση αποτελεσματικών ελέγχων πρόσβασης, ιδίως ό,τι έχει να κάνει με τη χρήση συνθηματικών και την ασφάλεια του εξοπλισμού χρήστη.

1. <u>*Χρήση συνθηματικού:*</u> οι χρήστες πρέπει να ακολουθούν μία σωστή πρακτική σε ό,τι αφορά την επιλογή και χρήση των συνθηματικών, όπως: α)να τηρούν τα συνθηματικά εμπιστευτικά, β) να αποφεύγουν την καταγραφή των συνθηματικών είτε σε χαρτί είτε σε κάποιο ηλεκτρονικό αρχείο, γ) τακτική αλλαγή των συνθηματικών τους, δ) να επιλέγουν συνθηματικά που να μπορούν να τα απομνημονεύσουν, αλλά να μην χρησιμοποιούν στοιχεία που κάποιος να μπορεί να μαντέψει (π.χ. ονόματα, τηλεφωνικούς αριθμούς, ημερομηνία γέννησης κλπ), να μην είναι κάποια λέξη, αλλά να αποτελείται από γράμματα και αριθμούς ή και σύμβολα, στ) να αποφεύγουν επαναχρησιμοποίηση ή ανακύκλωση παλιών κωδικών, ζ) να μη χρησιμοποιούν τα ίδια συνθηματικά που χρησιμοποιούν και στην προσωπική τους ζωή.

2. <u>Εξοπλισμός χωρίς επίβλεψη:</u> οι χρήστες θα πρέπει να τερματίζουν τις ενεργές συνεδρίες όταν και να αποσυνδέονται από τους υπολογιστές, εξυπηρετητές όταν ολοκληρώνουν την εργασία τους και γενικά να διασφαλίζουν την προστασία του πληροφοριακού και τηλεπικοινωνιακού εξοπλισμού που δεν επιτηρείται.
3. <u>Πολιτική καθαρού γραφείου και καθαρής οθόνης:</u> πρέπει να υιοθετηθεί μία πολιτική καθαρού γραφείου (για έντυπα και φορητά μέσα αποθήκευσης) και οθόνης (π.χ. screen saver με χρήση συνθηματικού για την πρόσβαση ή αποσύνδεση). Μία τέτοια πολιτική μειώνει τους κινδύνους μη εξουσιοδοτημένης πρόσβασης, απώλειας και καταστροφής πληροφορίας κατά τη διάρκεια αλλά κυρίως εκτός ωραρίου εργασίας. Επίσης, η χρήση φωτοαντιγραφικών μηχανημάτων και εκτυπωτών θα πρέπει να γίνεται με κωδικό ασφαλείας.

2.9.4 Έλεγχος πρόσβασης δικτύων

Η πρόσβαση τόσο στις εσωτερικές όσο και εξωτερικές δικτυακές υπηρεσίες πρέπει να ελέγχεται. Η πρόσβαση στα δίκτυα και τις δικτυακές υπηρεσίες δεν πρέπει να διακινδυνεύει την ασφάλεια, και γι' αυτό το λόγο θα πρέπει να υπάρχουν κατάλληλες διεπαφές μεταξύ των δικτύων του οργανισμού και των δικτύων που ανήκουν σε άλλους οργανισμούς ή δημόσιων δικτύων και να εφαρμόζονται κατάλληλοι μηχανισμοί εξουσιοδότησης στους χρήστες και στον εξοπλισμό.

1. <u>Πολιτική χρήσης των δικτυακών υπηρεσιών:</u> θα πρέπει να διατυπωθεί μία πολιτική σχετικά με τη χρήση των δικτύων και των δικτυακών υπηρεσιών, η οποία θα περιλαμβάνει α)τα δίκτυα και τις δικτυακές υπηρεσίες στα οποία επιτρέπεται η πρόσβαση, β)διαδικασίες εξουσιοδότησης για τον καθορισμό των χρηστών που έχουν πρόσβαση και για ποια δίκτυα και υπηρεσίες την έχουν, γ)διοικητικούς ελέγχους και διαδικασίες για προστασία της πρόσβασης, δ)τα μέσα που χρησιμοποιούνται για την πρόσβαση, π.χ. οι προϋποθέσεις για να επιτραπεί η πρόσβαση μέσω ενός παρόχου υπηρεσιών διαδικτύου ή σε ένα απομακρυσμένο σύστημα.
2. <u>Αυθεντικοποίηση χρηστών από εξωτερικές συνδέσεις:</u> η αυθεντικοποίηση των απομακρυσμένων χρηστών μπορεί να επιτευχθεί χρησιμοποιώντας, για παράδειγμα, μία τεχνική κρυπτογράφησης, διακριτικά υλικού (hardware tokens) ή ένα πρωτόκολλο πρόκλησης/απόκρισης (challenge/response protocol). Αντίστοιχες υλοποιήσεις αυτών των τεχνικών μπορούν να βρεθούν σε διάφορες λύσεις εικονικών ιδιωτικών δικτύων (VPNs). Εάν είναι δυνατόν, θα μπορούσε να χρησιμοποιηθεί ένα ιδιωτικό δίκτυο γραμμών ώστε να εξασφαλίζεται η πηγή της σύνδεσης. Επίσης, με τη χρήση διαδικασιών επανάκλησης, π.χ. χρησιμοποιώντας μόντεμ με δυνατότητα επανάκλησης (dial-back modems), επιτυγχάνεται η προστασία απέναντι σε μη εξουσιοδοτημένες και ανεπιθύμητες συνδέσεις με τα ΠΣ του οργανισμού. Με αυτό τον τρόπο αυθεντικοποιείται ο χρήστης που προσπαθεί να συνδεθεί με το δίκτυο του οργανισμού απομακρυσμένα. Αυτό επιτυγχάνεται με τον εξυπηρετητή να διακόπτει τη σύνδεση με τον απομακρυσμένο υπολογιστή και να εκτελεί νέα κλήση επιβεβαιώνοντας ότι πρόκειται για τον ίδιο υπολογιστή.
3. <u>Ταυτοποίηση δικτυακού εξοπλισμού:</u> η διαδικασία αυτή μπορεί να χρησιμοποιηθεί στη περίπτωση που η επικοινωνία μπορεί να ξεκινήσει από μία συγκεκριμένη τοποθεσία ή εξοπλισμό. Μία συσκευή αναγνώρισης που προσαρτάται στον εξοπλισμό μπορεί να δείξει κατά πόσο αυτός ο εξοπλισμός επιτρέπεται να συνδεθεί στο δίκτυο. Αυτές οι συσκευές θα πρέπει να υποδεικνύουν και σε ποια δίκτυα επιτρέπεται η σύνδεση, εάν υπάρχουν πάνω από ένα δίκτυα και ιδίως όταν διαφέρουν ως προς την ευαισθησία τους.
4. <u>Απομακρυσμένη διαχείριση και προστασία δικτυακών θυρών:</u> πρέπει να ελέγχεται η φυσική και λογική πρόσβαση στις θύρες (diagnostic, configuration ports). Πολλά υπολογιστικά και πληροφοριακά συστήματα εγκαθίστανται με δυνατότητα απομακρυσμένης διάγνωσης και διαμόρφωσης από τους τεχνικούς/μηχανικούς συντήρησης. Εάν αυτές οι θύρες επικοινωνίας μείνουν χωρίς προστασία συνιστούν κίνδυνο μη εξουσιοδοτημένης πρόσβασης.
5. <u>Διαχωρισμός δικτύων:</u> μία μέθοδος ελέγχου ασφάλειας σε μεγάλα δίκτυα είναι η διαίρεσή τους σε επιμέρους λογικούς τομείς δικτύου, για παράδειγμα τομέας εσωτερικού και εξωτερικού δικτύου ενός οργανισμού με διαφορετικά ορισμένες περιμέτρους ασφαλείας. Οι τομείς πρέπει να ορισθούν σύμφωνα με μία ανάλυση επικινδυνότητας και τις διαφορετικές απαιτήσεις ασφαλείας που πρέπει να έχει ο κάθε τομέας. Θα μπορούσε δηλαδή, να υπάρχει μία πύλη που θα ελέγχει την

πρόσβαση και τη ροή πληροφορίας μεταξύ των δύο τομέων και θα λειτουργούσε ως ένα φίλτρο κυκλοφορίας ανάμεσά τους Ο διαχωρισμός των δικτύων θα πρέπει να βασιστεί στην αξία και την κατηγοριοποίηση της πληροφορίας που αποθηκεύεται ή επεξεργάζεται, το επίπεδο εμπιστοσύνης και τους τομείς της επιχειρηματικής δραστηριότητας προκειμένου να μειωθούν οι συνολικές επιπτώσεις από τη διακοπή μίας υπηρεσίας.

6. *Έλεγχος δικτυακής σύνδεσης:* η δυνατότητα σύνδεσης των χρηστών μπορεί να περιορισθεί μέσω δικτυακών πυλών που φιλτράρουν την κυκλοφορία βάση προκαθορισμένων κανόνων. Οι περιορισμοί σύνδεσης θα πρέπει να ισχύσουν σε εφαρμογές όπως, ηλεκτρονικό ταχυδρομείο, μεταφορά αρχείων, διαδραστική πρόσβαση κλπ.
7. *Έλεγχος δικτυακής δρομολόγησης:* πρέπει να εφαρμοσθούν μέτρα ελέγχου δρομολόγησης, ώστε να διασφαλισθεί ότι οι συνδέσεις και οι ροές πληροφορίας δεν παραβιάζουν την πολιτική ελέγχου πρόσβασης στις επιχειρησιακές εφαρμογές.

2.9.5 Έλεγχος πρόσβασης λειτουργικών συστημάτων

Η πρόσβαση στα λειτουργικά συστήματα πρέπει να επιτρέπεται μόνο σε εξουσιοδοτημένους χρήστες. Θα πρέπει να διασφαλίζεται η αυθεντικοποίηση των εξουσιοδοτημένων χρηστών, σύμφωνα με μία ορισμένη πολιτική ελέγχου πρόσβασης, η καταγραφή επιτυχημένων και μη προσπαθειών αυθεντικοποίησης του συστήματος, η καταγραφή της χρήσης ειδικών δικαιωμάτων συστήματος, ειδοποίηση σε περιπτώσεις παραβιάσεων των πολιτικών ασφαλείας συστήματος, η παροχή κατάλληλων μέσων αυθεντικοποίησης, και όταν είναι απαραίτητο ο περιορισμός τους χρόνου σύνδεσης.

1. *Ασφαλής διαδικασία σύνδεσης:* θα πρέπει α) να μην εμφανίζονται αναγνωριστικά συστήματος ή εφαρμογών έως ότου ολοκληρωθεί επιτυχώς η σύνδεση, β) να εμφανίζεται ένα γενικό προειδοποιητικό ότι η πρόσβαση στον υπολογιστή γίνεται μόνο από εξουσιοδοτημένους χρήστες, γ)να μην υπάρχει κάποιο βοηθητικό μήνυμα κατά τη διαδικασία σύνδεσης που θα μπορούσε να χρησιμοποιηθεί από μη εξουσιοδοτημένο χρήστη, δ) να υπάρχει όριο αποτυχημένων προσπαθειών σύνδεσης (π.χ. 3 προσπάθειες), ε) να υπάρχει μέγιστος και ελάχιστος επιτρεπόμενος χρόνος σύνδεσης και εάν αυτός ο χρόνος ξεπερνιέται να τερματίζεται αυτόματα η σύνδεση, στ) μόλις επιτευχθεί μία σύνδεση θα πρέπει να εμφανίζεται η ημερομηνία και ώρα της τελευταίας επιτυχημένης σύνδεσης, αλλά και κάθε πληροφορία αποτυχημένων προσπαθειών που μεσολάβησαν από την τελευταία σύνδεση, ζ)να μην εμφανίζεται ο κωδικός που εισάγεται και να αποφεύγεται η μετάδοση των κωδικών πρόσβασης στο δίκτυο σε μορφή απλού κειμένου.
2. *Ταυτοποίηση και αυθεντικοποίηση χρηστών:* όλοι οι χρήστες πρέπει να έχουν ένα μοναδικό αναγνωριστικό (user ID), μόνο για προσωπική τους χρήση, και θα πρέπει να επιλεγεί η κατάλληλη τεχνική αυθεντικοποίησης για να εξακριβώνεται η ταυτότητα του χρήστη. Τα μέτρα ελέγχου θα πρέπει να εφαρμόζονται για κάθε τύπο χρήστη (συμπεριλαμβανομένου του προσωπικού τεχνικής υποστήριξης, διαχειριστών δικτύου, προγραμματιστών συστημάτων και διαχειριστών βάσεων δεδομένων). Τα αναγνωριστικά χρηστών πρέπει να χρησιμοποιούνται για τον εντοπισμό του υπεύθυνου για κάθε δραστηριότητα.
3. *Σύστημα διαχείρισης συνθηματικών:* ένα σύστημα διαχείρισης συνθηματικών πρέπει α)να επιβάλει τη χρήση ατομικών αναγνωριστικών και κωδικών πρόσβασης για τη τήρηση της λογοδοσίας, β) να επιτρέπει στους χρήστες να επιλέγουν και αλλάζουν τους προσωπικούς κωδικούς πρόσβασης και να συμπεριλαμβάνει μία διαδικασία επιβεβαίωσης για την αποφυγή λαθών, γ)επιβολή μίας επιλογής ποιοτικών κωδικών, δ)επιβολή αλλαγής κωδικού πρόσβασης, ε)τήρηση αρχείου των παλιών κωδικών και αποτροπή επαναχρησιμοποίησης τους, στ) να μην εμφανίζουν τους κωδικούς στην οθόνη κατά την πληκτρολόγησή τους, ζ) αποθήκευση των αρχείων κωδικών πρόσβασης χωριστά από τα δεδομένα εφαρμογών συστήματος η)αποθήκευση και μετάδοση των κωδικών πρόσβασης σε προστατευμένη (π.χ. κρυπτογραφημένη ή κατακερματισμένη) μορφή.
4. *Χρήση εργαλείων συστήματος:* η χρήση των εργαλείων συστήματος που μπορούν να παρακάμψουν τα μέτρα προστασίας (συστήματος και εφαρμογών) πρέπει να περιορίζεται και να ελέγχεται αυστηρά. Οι περισσότερες υπολογιστικές εγκαταστάσεις έχουν ένα ή περισσότερα

εργαλεία συστήματος τα οποία έχουν τη δυνατότητα να παρακάμπτουν τα μέτρα ελέγχου του συστήματος και των εφαρμογών. Θα πρέπει λοιπόν: α)να χρησιμοποιούνται διαδικασίες ταυτοποίησης, αυθεντικοποίησης και εξουσιοδότησης για τη χρήση των εργαλείων συστήματος, β) να γίνεται διαχωρισμός των εργαλείων συστήματος από το λογισμικό εφαρμογών, γ) να περιορίζεται η χρήση τους στον ελάχιστο απαιτούμενο αριθμό αξιόπιστων και εξουσιοδοτημένων χρηστών, δ) να απαιτείται εξουσιοδότηση για την κατά περίπτωση (ad hoc) χρήση τους, ε) να περιορίζεται η διαθεσιμότητά τους, και στ)να ορίζονται και τεκμηριώνονται τα επίπεδα εξουσιοδότησής.

5. *Λήξη συνεδρίας:* οι ανενεργές συνεδρίες πρέπει να τερματίζονται μετά το πέρας ενός προκαθορισμένου χρονικού διαστήματος. Ειδικά σε σημεία υψηλού κινδύνου, όπως δημόσιες ή εξωτερικές περιοχές που δεν προστατεύονται από τη διαχείριση ασφαλείας του οργανισμού, η εφαρμογή αντίστοιχων μέτρων ελέγχου είναι πολύ σημαντική. Οι συνεδρίες πρέπει να τερματίζουν για την αποτροπή εισόδου μη εξουσιοδοτημένων χρηστών και αποφυγή επιθέσεων στις υπηρεσίες.
6. *Περιορισμός χρόνου σύνδεσης:* απαραίτητη είναι η λήψη μέτρων ελέγχου του χρόνου σύνδεσης, ιδίως σε ευαίσθητες υπολογιστικές εφαρμογές. Για παράδειγμα α) χρήση προκαθορισμένων χρονικών θυρίδων για μετάδοση αρχείων δέσμης (batch files) ή τακτικών διαδραστικών συνεδριών μικρής διάρκειας, β)περιορισμό των χρόνων σύνδεσης στις ώρες γραφείου εάν δεν υπάρχει απαίτηση για εκτεταμένες ώρες λειτουργίας και γ) εξέταση εκ νέου εξουσιοδότησης σε τακτά χρονικά διαστήματα. Περιορίζοντας την περίοδο κατά την οποία επιτρέπονται συνδέσεις στις υπηρεσίες μειώνεται το περιθώριο ευκαιριών για μη εξουσιοδοτημένη πρόσβαση. Περιορίζοντας τη διάρκεια των ενεργών συνεδριών δεν επιτρέπεις στους χρήστες να έχουν ανοιχτές συνεδρίες και αποφεύγεται η εκ νέου εξουσιοδότηση.

2.9.6 Έλεγχος πρόσβασης στις εφαρμογές και την πληροφορία

Η λογική πρόσβαση στο λογισμικό και την πληροφορία των εφαρμογών πρέπει να περιορίζεται σε εξουσιοδοτημένους χρήστες μόνο. Τα συστήματα εφαρμογών θα πρέπει: α)να ελέγχουν την πρόσβαση στην πληροφορία και στις λειτουργίες τους, σύμφωνα με μια ορισμένη πολιτική ελέγχου πρόσβασης, β) να παρέχουν προστασία απέναντι σε μία μη εξουσιοδοτημένη πρόσβαση από οποιοδήποτε εργαλείο, λειτουργικό σύστημα ή κακόβουλο λογισμικό που έχει τη δυνατότητα να παρακάμψει το σύστημα ή τα μέτρα ελέγχου της εφαρμογής, και γ) να μην θέτουν σε κίνδυνο άλλα συστήματα με τα οποία μοιράζονται πληροφοριακούς πόρους.

1. *Περιορισμός πρόσβασης σε πληροφορίες:* οι περιορισμοί στην πρόσβαση πρέπει να βασίζονται στις ιδιαίτερες απαιτήσεις των επιχειρησιακών εφαρμογών. Η πολιτική ελέγχου πρόσβασης θα πρέπει να είναι σύμμορφη με την οργανωσιακή πολιτική πρόσβασης. Για την υποστήριξη των απαιτήσεων περιορισμού πρόσβασης θα πρέπει: α) να υπάρχουν μενού που θα ελέγχουν την πρόσβαση στις λειτουργίες του συστήματος εφαρμογής, β) να ελέγχονται τα δικαιώματα πρόσβασης των χρηστών (π.χ. ανάγνωση, εγγραφή, διαγραφή και εκτέλεση), γ) να ελέγχονται τα δικαιώματα πρόσβασης άλλων εφαρμογών, δ) να διασφαλίζεται ότι τα αποτελέσματα των συστημάτων εφαρμογών που χειρίζονται ευαίσθητη πληροφορία, περιέχουν μόνο τη σχετική πληροφορία για τη χρήση του αποτελέσματος και ότι αποστέλλονται σε εξουσιοδοτημένα τερματικά και τοποθεσίες.
2. *Απομόνωση ευαίσθητων συστημάτων:* τα ευαίσθητα συστήματα πρέπει να βρίσκονται σε ένα απομονωμένο υπολογιστικό περιβάλλον. Η ευαισθησία μίας εφαρμογής συστήματος θα πρέπει να προσδιορισθεί και τεκμηριωθεί από τον 'ιδιοκτήτη' της εφαρμογής. Όταν μία ευαίσθητη εφαρμογή πρόκειται να εκτελεσθεί σε κοινό περιβάλλον, τα συστήματα με τα οποία θα μοιρασθεί πόρους και οι ενδεχόμενοι κίνδυνοι θα πρέπει να εντοπισθούν, και να γίνουν αποδεχτά από τον 'ιδιοκτήτη' αυτής. Λόγω της ιδιαίτερης ευαισθησίας ορισμένων εφαρμογών σε πιθανή απώλεια, θα πρέπει να εκτελούνται σε ένα ξεχωριστό υπολογιστή και να μοιράζονται πόρους μόνο με συστήματα εμπιστοσύνης. Η απομόνωση μπορεί να επιτευχθεί χρησιμοποιώντας φυσικές και λογικές μεθόδους.

2.9.7 Απομακρυσμένη πρόσβαση και τηλεργασία

Η απαιτούμενη προστασία θα πρέπει να είναι ανάλογη με τους κινδύνους που αυτές οι ειδικές μορφές εργασίας αντιμετωπίζουν. Στην απομακρυσμένη πρόσβαση θα πρέπει να εξετάζονται οι κίνδυνοι της εργασίας σε ένα απροστάτευτο περιβάλλον και να εφαρμόζονται κατάλληλα μέτρα προστασίας. Στην περίπτωση της τηλεργασίας, ο οργανισμός θα πρέπει να εφαρμόζει τα κατάλληλα μέτρα προστασίας στο χώρο της τηλεργασίας και να διασφαλίζει ότι έχουν γίνει οι κατάλληλες ρυθμίσεις για αυτό τον τρόπο εργασίας.

1. *Απομακρυσμένη πρόσβαση και επικοινωνίες:* όταν γίνεται χρήση κινητών υπολογιστικών και επικοινωνιακών μονάδων, όπως για παράδειγμα φορητοί υπολογιστές, υπολογιστές χειρός, έξυπνες κάρτες, κινητά τηλέφωνα, θα πρέπει να υπάρχει ειδική μέριμνα που να διασφαλίζει ότι οι επιχειρησιακές πληροφορίες δε διακινδυνεύονται. Η πολιτική απομακρυσμένης πρόσβασης πρέπει να λαμβάνει υπόψη της τους κινδύνους της εργασίας με κινητό υπολογιστικό εξοπλισμό σε απροστάτευτα περιβάλλοντα. Η πολιτική αυτή θα πρέπει να συμπεριλαμβάνει, απαιτήσεις για φυσική προστασία, ελέγχους πρόσβασης, τεχνικές κρυπτογράφησης, λήψη αντιγράφων ασφαλείας και προστασία από ιούς. Επίσης, θα πρέπει να περιλαμβάνει κανόνες και συμβουλές για τη σύνδεση των κινητών μονάδων στα δίκτυα και οδηγίες για τη χρήση τους σε δημόσιους χώρους. Οι απομακρυσμένες συνδέσεις σε ασύρματα δίκτυα μπορεί να είναι παρόμοιες με άλλους τύπους συνδέσεων, αλλά έχουν ορισμένες σημαντικές διαφορές που θα πρέπει να λαμβάνονται υπόψη στα μέτρα προστασίας, όπως α)ότι ορισμένα πρωτόκολλα ασφάλειας για ασύρματες επικοινωνίες είναι ανώριμα και έχουν γνωστές αδυναμίες, και β) ύπαρξη κινδύνου μη δημιουργίας αντιγράφων ασφαλείας της αποθηκευμένης πληροφορίας στους φορητούς υπολογιστές, εξαιτίας του περιορισμένου εύρους ζώνης δικτύου, αλλά και αδυναμίας σύνδεσης του φορητού εξοπλισμού κατά το χρόνο που αυτά έχουν προγραμματισθεί.
2. *Τηλεργασία:* η τηλεργασία χρησιμοποιεί την τεχνολογία των επικοινωνιών ώστε να επιτευχθεί η απομακρυσμένη εργασία του προσωπικού από μία σταθερή τοποθεσία εκτός του οργανισμού. Θα πρέπει να προσδιορισθεί το είδος της εργασίας που επιτρέπεται, οι ώρες εργασίας και τα εσωτερικά συστήματα και υπηρεσίες που ο υπάλληλος έχει εξουσιοδοτημένη πρόσβαση. Επίσης, θα πρέπει να παρέχεται ο κατάλληλος εξοπλισμός επικοινωνίας, συμπεριλαμβανομένων των μεθόδων ασφαλείας της απομακρυσμένης πρόσβασης. Τέλος, θα πρέπει να παρέχεται το υλικό και λογισμικό υποστήριξης και συντήρησης, καθώς και ασφάλιση για όλο τον εξοπλισμό.

2.10 Προμήθεια, ανάπτυξη και συντήρηση πληροφοριακών συστημάτων

2.10.1 Απαιτήσεις ασφαλείας πληροφοριακών συστημάτων

Τα ΠΣ περιλαμβάνουν τα λειτουργικά συστήματα, τις πληροφοριακές υποδομές, τις επιχειρησιακές εφαρμογές, υπηρεσίες, εφαρμογές ανεπτυγμένες από τους χρήστες και έτοιμα προϊόντα πληροφορικής. Ο σχεδιασμός και η ανάπτυξη των ΠΣ για την υποστήριξη της επιχειρησιακής διαδικασίας είναι κρίσιμα στοιχεία για την ασφάλεια. Οι απαιτήσεις ασφαλείας θα πρέπει να εντοπίζονται κατά τη φάση καθορισμού των απαιτήσεων ενός έργου και να δικαιολογούνται, συμφωνούνται και τεκμηριώνονται ως αναπόσπαστο μέρος της συνολικής επιχειρησιακής περίπτωσης ενός ΠΣ.

1. *Ανάλυση απαιτήσεων και προδιαγραφών ασφαλείας:* οι ανάλυση απαιτήσεων για νέα ΠΣ ή για βελτιώσεις σε ήδη υπάρχοντα θα πρέπει να περιλαμβάνουν και απαιτήσεις για την ασφάλεια τους. Οι απαιτήσεις για μέτρα ελέγχου θα πρέπει να εξετάζουν τόσο τη χρήση αυτοματοποιημένων ελέγχων που είναι ενσωματωμένοι στα ΠΣ, όσο και την ανάγκη υποστήριξης μη αυτόματων ελέγχων. Ανάλογα κριτήρια θα πρέπει να υπάρχουν και κατά την αξιολόγηση πακέτων λογισμικού, που έχουν αναπτυχθεί ή αγορασθεί για επιχειρησιακές εφαρμογές. Οι απαιτήσεις ασφαλείας πρέπει να ενσωματώνονται στα πρώτα στάδια των έργων πληροφορικής. Μέτρα ελέγχου που εισάγονται στη φάση του σχεδιασμού έχουν σημαντικά μικρότερο κόστος ανάπτυξης και συντήρησης σε σχέση με αυτά που εισάγονται κατά τη διάρκεια ή μετά την υλοποίηση. Για τα

προϊόντα που αγοράζονται θα πρέπει να ακολουθείται μία τυπική διαδικασία δοκιμής και οι απαιτήσεις ασφαλείας θα πρέπει να αναφέρονται στο συμβόλαιο που συνάπτεται με τον προμηθευτή.

2.10.2 Ορθή επεξεργασία στις εφαρμογές

Θα πρέπει να ληφθούν κατάλληλα μέτρα ελέγχου στις εφαρμογές, συμπεριλαμβανομένων και αυτών που έχουν αναπτυχθεί από τους χρήστες για τη διασφάλιση της ορθής επεξεργασίας της πληροφορίας. Με αυτά τα μέτρα ελέγχου θα πρέπει να γίνεται επαλήθευση των δεδομένων εισόδου, της εσωτερικής επεξεργασίας και των δεδομένων εξόδου. Πρόσθετα μέτρα ελέγχου θα πρέπει να υφίστανται για συστήματα που επεξεργάζονται ή έχουν κάποιον αντίκτυπο σε ευαίσθητη, πολύτιμη και κρίσιμη πληροφορία. Ο καθορισμός αυτών των μέτρων ελέγχου θα γίνεται στο στάδιο του καθορισμού των απαιτήσεων ασφαλείας και της αξιολόγησης κινδύνου.

1. *Επαλήθευση δεδομένων εισόδου:* τα δεδομένα εισόδου των εφαρμογών πρέπει να επαληθεύονται ώστε να διασφαλίζεται ότι είναι τα ορθά και κατάλληλα δεδομένα. Η επαλήθευση μπορεί να γίνεται με τη χρήση μεθόδων όπως διπλή εισαγωγή δεδομένων ή έλεγχος ορίων, και χρήση περιορισμένων τιμών εισόδου σε ορισμένα πεδία για τον εντοπισμό τυχόν λαθών (δεδομένα εκτός του εύρους τιμών, μη έγκαιροι χαρακτήρες σε κάποια πεδία, ελλιπή δεδομένα, υπέρβαση του ανώτατου ή κατώτατου όγκου δεδομένων). Επίσης, συνίσταται η διενέργεια περιοδικών ελέγχων για την εγκυρότητα των περιεχομένων πεδίων-κλειδιών ή των αρχείων δεδομένων, αλλά και δημιουργία αρχείων καταγραφής (log files) των ενεργειών που συμμετέχουν στη διαδικασία εισαγωγής δεδομένων.
2. *Έλεγχος εσωτερικής επεξεργασίας:* δεδομένα που έχουν εισαχθεί σωστά μπορούν να αλλοιωθούν από σφάλματα υλικού, σφάλματα επεξεργασίας ή από εσκεμμένες ενέργειες. Οι έλεγχοι επαλήθευσης που πρέπει να γίνουν, είναι ανάλογοι της φύσης της εφαρμογής και των επιπτώσεων που θα έχει οποιαδήποτε αλλοίωση των δεδομένων στην επιχειρησιακή συνέχεια. Ο σχεδιασμός και υλοποίηση των εφαρμογών πρέπει να διασφαλίζει ότι οι κίνδυνοι από αστοχίες στην επεξεργασία, που οδηγούν σε απώλεια ακεραιότητας, ελαχιστοποιούνται. Συνίσταται η ύπαρξη μέτρων ελέγχου για τη διασφάλιση της εκτέλεσης των εφαρμογών στο σωστό χρόνο και με τη σωστή σειρά, αλλά και σε περίπτωση αστοχίας να τερματίζεται η εκτέλεση και διακόπτεται κάθε άλλη επεξεργασία μέχρι την επίλυση του προβλήματος. Τέλος, απαραίτητη είναι η χρησιμοποίηση προγραμμάτων επαναφοράς μετά από αστοχίες για τη διασφάλιση της ορθής επεξεργασίας των δεδομένων.
3. *Ακεραιότητα μηνύματος:* θα πρέπει να γίνει μία αξιολόγηση των κινδύνων και να ληφθούν τα κατάλληλα μέτρα για τη διατήρηση της αυθεντικότητας και ακεραιότητας των μηνυμάτων στις εφαρμογές.
4. *Επαλήθευση δεδομένων εξόδου:* η υλοποίηση συστημάτων και εφαρμογών συνήθως βασίζεται στην υπόθεση ότι εάν έχει γίνει σωστά η είσοδος των δεδομένων και η επεξεργασία τους, τότε η έξοδος θα είναι πάντα σωστή. Ωστόσο, η υπόθεση αυτή δεν ισχύει πάντα, και συστήματα που έχει γίνει δοκιμή της λειτουργίας τους, μπορούν κάτω από ορισμένες συνθήκες να παράγουν λάθος αποτέλεσμα. Οπότε, θα πρέπει να ληφθούν κατάλληλα μέτρα ελέγχου και για τη διασφάλιση ότι τα δεδομένα εξόδου μίας εφαρμογής, προκύπτουν από τη σωστή επεξεργασία της αποθηκευμένης πληροφορίας. Συστήνεται η εφαρμογή ελέγχων 'αληθοφάνειας', για τη διαπίστωση ότι τα δεδομένα εξόδου είναι εύλογα και αναμενόμενα.

2.10.3 Χρήση κρυπτογραφικών μεθόδων

Η εμπιστευτικότητα, αυθεντικότητα και ακεραιότητα των πληροφοριών πρέπει να προστατεύεται με κρυπτογραφικές μεθόδους. Πρέπει να αναπτυχθεί και υλοποιηθεί μία συγκεκριμένη πολιτική για τη χρήση κρυπτογραφικών μεθόδων, ενώ παράλληλα θα πρέπει να γίνεται διαχείριση των κρυπτογραφικών κλειδιών.

1. *Πολιτική χρήσης κρυπτογραφικών μεθόδων:* η απόφαση για την καταλληλότητα μίας κρυπτογραφικής λύσης, αποτελεί μέρος της ευρύτερης διαδικασίας της εκτίμησης κινδύνων και

της επιλογής μέτρων ελέγχου. Η πολιτική χρήσης κρυπτογραφικών μεθόδων, είναι απαραίτητη για τη μεγιστοποίηση του οφέλους και ελαχιστοποίηση των ρίσκων από τη χρήση αυτών των μεθόδων, αλλά και για την αποφυγή ακατάλληλης και λανθασμένης χρήσης. Όταν γίνεται χρήση ψηφιακών υπογραφών, πρέπει να εξετάζεται η σχετική νομοθεσία, και πιο συγκεκριμένα αυτή που περιγράφει τις προϋποθέσεις υπό τις οποίες μία ψηφιακή υπογραφή είναι νομικά δεσμευτική. Η ανάπτυξη και υλοποίηση της πολιτικής θα πρέπει:

α) Να βασίζεται σε μία εκτίμηση επικινδυνότητας.
β) Να εντοπίζονται τα απαιτούμενα επίπεδα προστασίας, λαμβάνοντας υπόψη τον τύπο, τη δύναμη και την ποιότητα του αλγορίθμου κρυπτογράφησης που απαιτείται.
γ) Να εξετάζεται η διαδικασία της διαχείρισης κλειδιών, συμπεριλαμβανομένων των μεθόδων προστασίας των κρυπτογραφικών κλειδιών και την ανάκτηση της κρυπτογραφημένης πληροφορίας σε περίπτωση, απολεσθέντων, παραβιασθέντων ή κατεστραμμένων κλειδιών.
δ) Να εξετάζονται οι ευθύνες και τα καθήκοντα, για παράδειγμα της υλοποίησης της πολιτικής, της διαχείρισης ή της δημιουργίας των κλειδιών.
ε) Να εξετάζονται οι επιπτώσεις της χρήσης κρυπτογραφημένης πληροφορίας σε ελέγχους που βασίζονται στην επιθεώρηση του περιεχομένου.

Με τη χρήση κρυπτογραφικών μεθόδων επιτυγχάνονται η **εμπιστευτικότητα** (χρήση κρυπτογράφησης για την προστασία ευαίσθητης ή κρίσιμης πληροφορίας που είτε αποθηκεύεται είτε μεταφέρεται), η **ακεραιότητα/αυθεντικότητα** (χρήση ψηφιακών υπογραφών ή κωδικών αυθεντικοποίησης μηνυμάτων) και η **μη άρνηση της ευθύνης** (χρήση κρυπτογραφικών τεχνικών για την απόδειξη της παρουσίας ή όχι ενός γεγονότος ή μίας ενέργειας).

2. *Διαχείριση κλειδιών:* η διαχείριση των κρυπτογραφικών κλειδιών είναι βασική για την αποτελεσματική χρήση των κρυπτογραφικών τεχνικών. Υπάρχουν δύο τύποι τεχνικών:
   α) η τεχνική **μυστικού κλειδιού**, όπου δύο ή περισσότερα μέρη μοιράζονται ένα κοινό κλειδί, το οποίο χρησιμοποιείται τόσο για την κρυπτογράφηση όσο και αποκρυπτογράφηση της πληροφορίας. Αυτό το κλειδί πρέπει να παραμένει μυστικό αφού όποιος έχει πρόσβαση σε αυτό έχει τη δυνατότητα να αποκρυπτογραφήσει όλη την πληροφορία που έχει κρυπτογραφηθεί με αυτό το κλειδί, ή να εισάγει πληροφορία χωρίς εξουσιοδότηση.
   β) η τεχνική **δημόσιου κλειδιού**, όπου κάθε χρήστης έχει ένα ζευγάρι κλειδιών, ένα δημόσιο (που μπορεί να αποκαλυφθεί στον καθένα) και ένα ιδιωτικό (το οποίο παραμένει μυστικό). Αυτή η τεχνική χρησιμοποιείται συνήθως για κρυπτογράφηση και κυρίως για την παραγωγή ψηφιακών υπογραφών.

   Ένα σύστημα διαχείρισης κλειδιών πρέπει να βασίζεται σε ένα συμφωνημένο σύνολο προτύπων, διαδικασιών και ασφαλών μεθόδων για τη δημιουργία, διανομή, αποθήκευση, αλλαγή, ανανέωση, ανάκληση, ανάκτηση, αρχειοθέτηση και καταστροφή των κλειδιών. Πρέπει να ορίζεται το χρονικό διάστημα μέσα στο οποίο μπορούν να χρησιμοποιηθούν τα κλειδιά, το οποίο θα εξαρτάται από τους κατά περίπτωση κινδύνους. Οι συνεργασίες με εξωτερικούς παρόχους αντίστοιχων υπηρεσιών, π.χ. μία αρχή πιστοποίησης, θα πρέπει να εστιάζουν σε θέματα αξιοπιστίας, χρόνου απόκρισης και ανάληψης ευθυνών από αυτούς.

2.10.4 Ασφάλεια αρχείων συστήματος

Η πρόσβαση στα αρχεία συστήματος και τον πηγαίο κώδικα των προγραμμάτων πρέπει να ελέγχεται, όπως επίσης και τα έργα πληροφορικής και οι δραστηριότητες υποστήριξης να διεξάγονται με ασφαλή τρόπο. Τέλος, θα πρέπει να λαμβάνεται μέριμνα για την αποφυγή ευαίσθητων δεδομένων σε περιβάλλοντα δοκιμών.

1. *Έλεγχος λογισμικού:* οι ενημερώσεις του λογισμικού, των εφαρμογών και των βιβλιοθηκών των προγραμμάτων πρέπει να γίνονται από εκπαιδευμένους διαχειριστές. Τα λειτουργικά συστήματα πρέπει να αναβαθμίζονται μόνο όταν υπάρχει συγκεκριμένη απαίτηση, για παράδειγμα, εάν η τρέχουσα έκδοση δεν υποστηρίζει πλέον της επιχειρησιακές απαιτήσεις. Δεν θα πρέπει να γίνεται αναβάθμιση μόνο και μόνο επειδή μία νέα έκδοση του λειτουργικού συστήματος είναι διαθέσιμη, διότι μπορεί να είναι λιγότερο ασφαλή, σταθερή και κατανοητή από την τρέχουσα έκδοση.

«Μπαλώματα» λογισμικού (patches) πρέπει να εγκαθίστανται μόνο στην περίπτωση που κλείνουν απομακρύνουν ή μειώνουν τα κενά ασφαλείας και τα τρωτά σημεία της τρέχουσας έκδοσης. Το εμπορικό λογισμικό που χρησιμοποιείται θα πρέπει να υποστηρίζεται από τον προμηθευτή του. Ιδιαίτερη προσοχή πρέπει να δίδεται σε παλαιότερες εκδόσεις πακέτων λογισμικού για τις οποίες οι προμηθευτές παύουν να παρέχουν υποστήριξη. Για τη μείωση του κινδύνου εμφάνισης προβλημάτων των λειτουργικών συστημάτων, θα πρέπει: α)οι ενημερώσεις λογισμικού να εκτελούνται από εξουσιοδοτημένους εκπαιδευμένους διαχειριστές, β) τα λειτουργικά συστήματα πρέπει να τρέχουν μόνο εκτελέσιμο κώδικα και όχι κώδικα προγραμματισμού ή μεταγλώττιση προγραμμάτων, γ) να χρησιμοποιείται ένα σύστημα ελέγχου διαμόρφωσης, και δ) οι παλαιότερες εκδόσεις να αρχειοθετούνται, μαζί με όλη την απαιτούμενη πληροφορία, παραμέτρους και ρυθμίσεις για όσο διάστημα τηρούνται τα δεδομένα στο αρχείο.

2. <u>*Προστασία των δεδομένων ελέγχου του συστήματος:*</u> τα δοκιμαστικά δεδομένα πρέπει να συλλέγονται με προσοχή, να προστατεύονται και να ελέγχονται. Η χρησιμοποίηση βάσεων δεδομένων που περιέχουν προσωπικά δεδομένα ή οποιαδήποτε άλλη ευαίσθητη πληροφορία για δοκιμές ελέγχου πρέπει να αποφεύγεται. Οι δοκιμές συστημάτων και αποδοχής συνήθως απαιτούν δοκιμαστικά δεδομένα που να προσεγγίζουν όσο είναι δυνατό τα πραγματικά. Σε περίπτωση λοιπόν, που χρησιμοποιείται ευαίσθητη πληροφορία, αυτή θα πρέπει είτε να αφαιρείται είτε να τροποποιείται κατά τέτοιο τρόπο ώστε να μην μπορεί να αναγνωρισθεί.
3. <u>*Έλεγχος πρόσβασης στον πηγαίο κώδικα:*</u> η πρόσβαση στον πηγαίο κώδικα πρέπει να είναι περιορισμένη. Εάν είναι δυνατό οι βιβλιοθήκες δεν πρέπει να βρίσκονται στα λειτουργικά συστήματα, ενώ η συντήρησή και αντιγραφή τους θα υπόκειται σε αυστηρές διαδικασίες ελέγχου αλλαγών.

2.10.5 Ασφάλεια κατά την ανάπτυξη και συντήρηση

Τα στελέχη που είναι υπεύθυνα για τις εφαρμογές θα πρέπει να είναι έχουν την ευθύνη και για την ασφάλεια των έργων και του περιβάλλοντος υποστήριξης. Πρέπει να διασφαλίζουν ότι όλες οι προτεινόμενες αλλαγές των ΠΣ αξιολογούνται και δε θέτουν σε κίνδυνο την ασφάλεια είτε του συστήματος είτε του περιβάλλοντος λειτουργίας.

1. <u>*Διαδικασίες ελέγχου αλλαγών:*</u> μία καλή πρακτική είναι η δοκιμή του νέου λογισμικού σε ένα ξεχωριστό περιβάλλον τόσο από αυτό της παραγωγής όσο και αυτό της ανάπτυξης. Με αυτό τον τρόπο επιτυγχάνεται έλεγχος στο νέο λογισμικό και πρόσθετη προστασία της λειτουργικής πληροφορίας που χρησιμοποιείται για δοκιμαστικούς σκοπούς. Οι αυτόματες ενημερώσεις δεν πρέπει να χρησιμοποιούνται σε κρίσιμα συστήματα μιας και κάποιες από αυτές θα μπορούσαν να προκαλέσουν αποτυχία εκτέλεσης κρίσιμων εφαρμογών. Οι διαδικασίες θα πρέπει να περιλαμβάνουν: α) τήρηση αρχείου επιπέδων εξουσιοδότησης, β) διασφάλιση ότι μόνο εξουσιοδοτημένοι χρήστες υποβάλλουν αλλαγές, γ) εντοπισμός όλου του λογισμικού, πληροφορίας, βάσεων δεδομένων, υλικού που τροποποιείται, δ) διασφάλιση ότι ενημερώνεται η τεκμηρίωση του συστήματος μετά από κάθε αλλαγή, ε) τήρηση μίας έκδοσης ελέγχου για όλες τις ενημερώσεις λογισμικού και στ) τήρηση μίας διαδρομής ελέγχου για όλες τις αιτήσεις αλλαγής.
2. <u>*Τεχνική αναθεώρηση εφαρμογών μετά από αλλαγές στο λειτουργικό σύστημα:*</u> μετά από αλλαγές στο λειτουργικό σύστημα, οι κρίσιμες επιχειρησιακά εφαρμογές πρέπει να αναθεωρούνται και να δοκιμάζονται για τη διασφάλιση μη ύπαρξης παρενεργειών στη λειτουργία ή την ασφάλειά τους. Θα πρέπει να διασφαλίζεται ότι οι αναθεωρήσεις και οι δοκιμές του συστήματος που προκύπτουν έπειτα από αυτές τις αλλαγές, καλύπτονται από το ετήσιο σχέδιο στήριξης και προϋπολογισμό.
3. <u>*Περιορισμοί αλλαγών σε πακέτα λογισμικού:*</u> τα εμπορικά πακέτα λογισμικού πρέπει χρησιμοποιούνται χωρίς τροποποιήσεις. Εάν είναι απαραίτητη κάποια αλλαγή το πρωτότυπο λογισμικό θα πρέπει να τηρείται και αυτή πρέπει να εφαρμόζεται σε ένα ακριβές αντίγραφο του. όλες οι αλλαγές πρέπει να δοκιμάζονται και να τεκμηριώνονται πλήρως, ώστε να είναι δυνατή η επανεφαρμογή τους σε μελλοντικές αναβαθμίσεις του λογισμικού.
4. <u>*Διαρροή πληροφοριών:*</u> είναι δυνατή η ύπαρξη εντός του δικτύου ή των ΠΣ **μυστικών καναλιών** (covert channels), τα οποία είναι μονοπάτια που δεν προορίζονται για τη ροή της πληροφορίας. Για παράδειγμα ο δυφιακός χειρισμός (bit manipulation)σε πακέτα πρωτοκόλλων επικοινωνίας θα

μπορούσε να χρησιμοποιηθεί ως μία κρυφή μέθοδος μετάδοσης σήματος. Εκ φύσεως, η αποτροπή όλων των δυνατών μυστικών καναλιών θα ήταν αδύνατη, ωστόσο, συχνά γίνεται εκμετάλλευση τους π.χ. από κακόβουλα προγράμματα. Η λήψη μέτρων προστασίας από κακόβουλο κώδικα μειώνει και τους κινδύνους εκμετάλλευσης τους. Επίσης, συνίσταται η σάρωση των εξερχόμενων μέσων επικοινωνίας για κρυμμένη πληροφορία, η απόκρυψη της συμπεριφοράς των συστημάτων και επικοινωνιών για τη μείωση της πιθανότητας ένα τρίτο μέρος να είναι σε θέση να συνάγει πληροφορίες από αυτή τη συμπεριφορά, και συνεχή παρακολούθηση της χρήσης των πόρων των υπολογιστικών συστημάτων.

5. <u>*Ανάπτυξη λογισμικού με εξωτερική ανάθεση:*</u> η ανάθεση της ανάπτυξης λογισμικού σε τρίτους θα πρέπει να γίνεται υπό την επίβλεψη και τον έλεγχο του οργανισμού. Θα πρέπει να διευκρινίζονται ζητήματα όπως, α)δικαιώματα πνευματικής ιδιοκτησίας, β)συμφωνίες παραχώρησης αδειών λογισμικού γ)ιδιοκτησία του κώδικα, δ)πιστοποίηση της ποιότητας και ακρίβειας της προσφερόμενης εργασίας, ε)εγγυήσεις σε περίπτωση αποτυχίας του τρίτου μέρους, στ)δικαιώματα πρόσβασης για έλεγχο της ποιότητας και ακρίβειας της εργασίας, ζ)συμβατικές απαιτήσεις για την ποιότητα και ασφάλεια του κώδικα και η)δοκιμή πριν την εγκατάσταση για εντοπισμό κακόβουλου κώδικα.

2.10.6 Διαχείριση τεχνικών ευπαθειών

Η διαχείριση των τεχνικών ευπαθειών πρέπει να εφαρμόζεται κατά τρόπο αποτελεσματικό, συστηματικό και επαναλαμβανόμενο, με στόχο τη μείωση των κινδύνων που προκύπτουν από την εκμετάλλευση δημοσιοποιημένων ευπαθειών. Η διαχείριση πρέπει να περιλαμβάνει τα λειτουργικά συστήματα και οποιαδήποτε εφαρμογή χρησιμοποιείται.

1. <u>*Έλεγχος τεχνικών ευπαθειών:*</u> η σωστή λειτουργία της διαχείρισης των τεχνικών ευπαθειών ενός οργανισμού είναι κρίσιμη και θα πρέπει να παρακολουθείται. Θα πρέπει να λαμβάνεται έγκαιρη πληροφόρηση σχετικά με τις τεχνικές αδυναμίες των ΠΣ του οργανισμού, να εκτιμάται ο βαθμός της έκθεσής τους σε αυτές τις ευπάθειες και να λαμβάνονται κατάλληλα μέτρα για την αντιμετώπισή τους. Η πληροφόρηση μεταξύ άλλων πρέπει να περιλαμβάνει τους προμηθευτές λογισμικού, την έκδοση, την τρέχουσα κατάσταση (τι λογισμικό είναι ήδη εγκατεστημένο και σε ποια συστήματα) και τον υπεύθυνο εντός του οργανισμού για το λογισμικό. Μία πλήρης καταγραφή των αγαθών είναι απαραίτητη προϋπόθεση για την αποτελεσματική διαχείριση των τεχνικών ευπαθειών. Μόλις μία ευπάθεια γίνει αντιληπτή, ο οργανισμός θα πρέπει να εντοπίσει τους κινδύνους και τα μέτρα που πρέπει να ληφθούν, όπως για παράδειγμα εγκατάσταση «μπαλωμάτων» (patches) στα ευπαθή συστήματα. Εάν υπάρχει διαθέσιμο κάποιο «μπάλωμα», θα πρέπει να εξετάζονται οι κίνδυνοι που προκύπτουν από την εγκατάστασή του (δηλαδή πρέπει να γίνει σύγκριση μεταξύ της ευπάθειας και των κινδύνων από την εγκατάσταση). Εάν δεν υπάρχει διαθέσιμο κάποιο «μπάλωμα» θα πρέπει να εξετασθούν άλλα μέτρα, όπως, απενεργοποίηση των υπηρεσιών που σχετίζονται με την ευπάθεια, προσαρμογή ή προσθήκη ελέγχων πρόσβασης, αυξημένη παρακολούθηση για τον εντοπισμό και αποτροπή πραγματικών επιθέσεων και μία ιεράρχηση των ευπαθειών, π.χ. τα υψηλού κινδύνου συστήματα πρέπει να αντιμετωπίζονται πρώτα.

2.11 Διαχείριση περιστατικών ασφαλείας

2.11.1 Αναφορά περιστατικών και αδυναμιών

Τα περιστατικά ασφαλείας και αδυναμίες που σχετίζονται με τα ΠΣ πρέπει να αναφέρονται σε εξουσιοδοτημένο σημείο αναφοράς (designated point of contact), ώστε να διασφαλισθεί η έγκαιρη αντιμετώπισή τους. Σημείο αναφοράς μπορεί να αποτελεί ο Υπεύθυνος Ασφαλείας ΠΣ του οργανισμού. Για το σκοπό αυτό πρέπει να υπάρχουν σαφείς και καταγεγραμμένες διαδικασίες για την αναφορά και τη διερεύνησή τους, οι οποίες πρέπει να γνωστοποιούνται σε όλο το προσωπικό και εξωτερικούς συνεργάτες.

1. <u>Αναφορά περιστατικών:</u> τα περιστατικά παραβίασης ασφαλείας των ΠΣ πρέπει να αναφέρονται άμεσα μέσω κατάλληλων καναλιών επικοινωνίας. Θα πρέπει να υπάρχει μία επίσημη διαδικασία αναφοράς περιστατικών παραβίασης ασφαλείας, σε συνδυασμό με μία διαδικασία κλιμάκωσης και αντιμετώπισης των περιστατικών, η οποία θα καθορίζει τις ενέργειες που πρέπει να γίνουν. Επίσης, θα πρέπει να ορισθεί ένα σημείο αναφοράς (point of contact) για την αναφορά των περιστατικών, το οποίο πρέπει να είναι ένα πρόσωπο γνωστό εντός του οργανισμού, το οποίο είναι διαθέσιμο και παρέχει άμεση απόκριση κάθε στιγμή. Για την υποστήριξη της διαδικασίας, συστήνεται η χρήση εντύπων αναφορών, για υποβοήθηση του προσωπικού να λάβει όλες τις απαραίτητες ενέργειες σε περίπτωση περιστατικού. Η σωστή συμπεριφορά σε περίπτωση περιστατικού ασφαλείας είναι η σημείωση κάθε σημαντικής λεπτομέρειας και αποφυγή κάθε προσωπικής ενέργειας, αλλά άμεση ενημέρωση στο σημείο αναφοράς. Ορισμένα παραδείγματα περιστατικών ασφαλείας είναι α)απώλεια υπηρεσιών , εξοπλισμού ή εγκαταστάσεων, β)δυσλειτουργία ή υπερφόρτωση συστήματος, γ)ανθρώπινα λάθη, δ)μη συμμόρφωση με πολιτικές και οδηγίες, ε)κενά φυσικής ασφάλειας, στ)αλλαγές συστήματος χωρίς έλεγχο, ζ)δυσλειτουργίες στο λογισμικό ή υλικό και η)παραβιάσεις πρόσβασης. Τα περιστατικά ασφαλείας, μπορούν να χρησιμοποιηθούν στην εκπαίδευση και ευαισθητοποίηση των χρηστών, ως παραδείγματα τα οποία θα μπορούσαν να συμβούν κατά την εργασία τους, πως θα έπρεπε να ενεργήσουν και πως θα τα αποφύγουν στο μέλλον.
2. <u>Αναφορά ευπαθειών συστήματος:</u> το προσωπικό και οι συνεργάτες του οργανισμού που χρησιμοποιούν τα ΠΣ και τις υπηρεσίες θα πρέπει να καταγράφουν και αναφέρουν, κάθε ευπάθεια ασφαλείας που τυχόν παρατηρούν ή υποπτεύονται, στο προϊστάμενό τους ή απευθείας στον πάροχο της υπηρεσίας.

2.11.2 Διαχείριση περιστατικών και διορθωτικές κινήσεις

Οι αρμοδιότητες και οι διαδικασίες που σχετίζονται με τη διαχείριση περιστατικών και ευπαθειών πρέπει να καθορίζονται. Η απόκριση, παρακολούθηση, αξιολόγηση και η συνολική διαχείριση των περιστατικών πρέπει να γίνεται με στόχο τη συνεχή βελτίωση. Η συλλογή τυχόν αποδεικτικών στοιχείων πρέπει πάντα να είναι σύμφωνη με τη νομοθεσία.

1. <u>Αρμοδιότητες και διαδικασίες:</u> α) οι διαδικασίες θα πρέπει να χειρίζονται τους διαφορετικούς τύπους περιστατικών, (αστοχίες των ΠΣ ή απώλεια υπηρεσιών, κακόβουλο λογισμικό, άρνηση υπηρεσιών, σφάλματα που προκύπτουν από ελλιπή ή ανακριβή επιχειρησιακά δεδομένα, κενά εμπιστευτικότητας και ακεραιότητας), β) πρόσθετα των σχεδίων έκτακτης ανάγκης πρέπει να γίνεται ανάλυση και προσδιορισμός της αιτίας του περιστατικού, περιορισμός, σχεδιασμός και εφαρμογή διορθωτικών ενεργειών, επικοινωνία με όσους έχουν πληγεί ή συμμετέχουν στην επαναφορά από το περιστατικό, και αναφορά στις αρμόδιες αρχές, γ)ίχνη και λοιπά αποδεικτικά στοιχεία πρέπει να συλλέγονται και ασφαλίζονται κατάλληλα για εσωτερική ανάλυση του προβλήματος, για τη χρήση ως ανακριτικού υλικού (forensic evidence) σε περίπτωση παραβίασης συμφωνίας, κανονισμών ή αστικών και ποινικών διώξεων, και για απαίτηση αποζημίωσης από τους προμηθευτές λογισμικού και υπηρεσιών, και δ) η διαδικασία επαναφοράς θα πρέπει να επιτρέπει μόνο σε εξουσιοδοτημένο προσωπικό την πρόσβαση σε επιζώντα ΠΣ και δεδομένα, να περιλαμβάνει λεπτομερή τεκμηρίωση και αξιολόγηση όλων των έκτακτων ενεργειών, και επιβεβαιώνει με την ελάχιστη καθυστέρηση την ακεραιότητα των ΠΣ και των μέτρων ελέγχου.
2. <u>Γνώση από τα περιστατικά:</u> οι πληροφορίες που αποκτούνται από την αξιολόγηση θα πρέπει να χρησιμοποιούνται για τον εντοπισμό επαναλαμβανόμενων και με σημαντικές επιπτώσεις περιστατικών. Η αξιολόγηση μπορεί να υποδεικνύει την ανάγκη για πρόσθετους ελέγχους με στόχο τον περιορισμό της συχνότητας και κόστους μελλοντικών συμβάντων ή να πρέπει να ληφθεί υπόψη στη διαδικασία αναθεώρησης της πολιτικής ασφαλείας.
3. <u>Συλλογή αποδεικτικών στοιχείων:</u> όταν εντοπίζεται ένα συμβάν ασφαλείας, σε πρώτη φάση μπορεί να μην είναι προφανές ότι θα καταλήξει σε προσφυγή στη δικαιοσύνη. Υπάρχει ο κίνδυνος, της σκόπιμης ή τυχαίας καταστροφής των αποδεικτικών στοιχείων, προτού γίνει αντιληπτή η σοβαρότητα του περιστατικού. Γι' αυτό το λόγο είναι σκόπιμη η συμμετοχή δικηγόρου ή των αστυνομικών αρχών στα πρώτα στάδια τυχόν νομικών ενεργειών για τη χορήγηση συμβουλών

σχετικά με τα αποδεικτικά στοιχεία που απαιτούνται. Συγκεκριμένα, δύο βασικοί κανόνες που πρέπει να λαμβάνονται υπόψη σε αυτές τις περιπτώσεις είναι α)το παραδεκτό των αποδεικτικών στοιχείων (δηλαδή εάν αυτά τα στοιχεία ευσταθούν σε δίκη) και β)η βαρύτητά τους (δηλαδή η ποιότητα και πληρότητα των στοιχείων). Για τη διασφάλιση του παραδεκτού των στοιχείων, τα ΠΣ του οργανισμού θα πρέπει να συμμορφώνονται με κάποιο επίσημο πρότυπο ή κώδικα πρακτικής.

2.12 Διαχείριση επιχειρησιακής συνέχειας

2.12.1 Ασφάλεια ΠΣ και επιχειρησιακή συνέχεια

Η διαχείριση της επιχειρησιακής συνέπειας πρέπει να εφαρμόζεται για τη μείωση του αντίκτυπου στον οργανισμό και την επαναφορά έπειτα από απώλεια πληροφοριακών αγαθών (τα οποία μπορεί να είναι αποτέλεσμα μίας φυσικής καταστροφής, ατυχημάτων, αστοχίας υλικού ή μιας εσκεμμένης ενέργειας) σε ένα αποδεκτό επίπεδο μέσω ενός συνδυασμού μέτρων πρόληψης και αποκατάστασης. Θα πρέπει να προσδιορισθούν οι κρίσιμες επιχειρησιακές διαδικασίες και να ενσωματωθούν στις απαιτήσεις ασφάλειας και επιχειρησιακής συνέχειας άλλων τομέων όπως λειτουργίες, προσωπικό, υλικά, μεταφορές και εγκαταστάσεις. Οι συνέπειες που προκύπτουν από καταστροφές, αποτυχίες ασφαλείας, απώλεια και διαθεσιμότητα υπηρεσίας, θα πρέπει να υπόκεινται σε μία ανάλυση επιπτώσεων προς τον οργανισμό. Πρέπει να αναπτυχθούν και εφαρμοσθούν σχέδια επιχειρησιακής συνέχειας για τη διασφάλιση της έγκαιρης επανέναρξης των βασικών λειτουργιών. Η ασφάλεια των ΠΣ θα πρέπει να αποτελεί αναπόσπαστο κομμάτι της συνολικής διαδικασίας επιχειρησιακής συνέχειας, καθώς και των άλλων διαδικασιών διαχείρισης του οργανισμού. Τέλος, θα πρέπει να λαμβάνονται μέτρα ελέγχου για τον εντοπισμό και μείωση των κινδύνων, τον περιορισμό των συνεπειών από καταστροφικά περιστατικά και τη διασφάλιση ότι η πληροφορία που απαιτείται για τις επιχειρησιακές διαδικασίες θα είναι άμεσα διαθέσιμη.

1. <u>Ενσωμάτωση ασφάλειας στην επιχειρησιακή συνέχεια:</u> η διαδικασία αυτή θα πρέπει να λάβει υπόψη τα εξής στοιχεία κλειδιά της διαχείρισης επιχειρησιακής συνέχειας: α) κατανόηση των κινδύνων που αντιμετωπίζει ο οργανισμός όσον αφορά την πιθανότητα και τις επιπτώσεις σε βάθος χρόνου, και εντοπισμός και ιεράρχηση των κρίσιμων επιχειρησιακών διαδικασιών, β)εντοπισμός όλων των αγαθών που εμπλέκονται στις κρίσιμες διαδικασίες, γ)κατανόηση των πιθανών επιπτώσεων στον οργανισμό από διακοπές που οφείλονται σε περιστατικά ασφαλείας και καθορισμός των επιχειρησιακών στόχων των ΠΣ (είναι σημαντικό να εντοπισθούν σοβαρά περιστατικά που θα μπορούσαν να απειλήσουν τη βιωσιμότητα του οργανισμού, αλλά και λύσεις που θα προκαλούν μικρότερες επιπτώσεις), δ)εξέταση αγοράς κατάλληλης ασφάλισης η οποία να αποτελεί μέρος της συνολικής επιχειρησιακής διαδικασίας, αλλά και κομμάτι της διαχείρισης λειτουργικών κινδύνων, ε)προσδιορισμός επαρκών οικονομικών, οργανωσιακών, τεχνικών και περιβαλλοντικών πόρων για κάλυψη των αναγνωρισμένων απαιτήσεων ασφαλείας, στ)διασφάλιση της ασφάλειας του προσωπικού και της προστασίας των πληροφοριακών υποδομών και περιουσίας του οργανισμού, ζ)διατύπωση και τεκμηρίωση των σχεδίων επιχειρησιακής συνέχειας σύμφωνα με τις απαιτήσεις ασφαλείας και τη γενικότερη στρατηγική, η)τακτικός έλεγχος και επικαιροποίηση των σχεδίων και διαδικασιών, και θ)ανάθεση της ευθύνης της διαδικασίας στο κατάλληλο επίπεδο διοίκησης του οργανισμού.
2. <u>Εκτίμηση επικινδυνότητας:</u> πρέπει να αναγνωρισθούν γεγονότα (ή ακολουθίες γεγονότων) που θα μπορούσαν να προκαλέσουν διακοπές στις επιχειρησιακές διαδικασίες του οργανισμού (π.χ. βλάβη εξοπλισμού, ανθρώπινα λάθη, κλοπή, πυρκαγιά, φυσικές καταστροφές και τρομοκρατικές ενέργειες). Ακολούθως, θα πρέπει να γίνει εκτίμηση της επικινδυνότητας για τον προσδιορισμό της πιθανότητας εμφάνισης του περιστατικού, των επιπτώσεων από τη διακοπή σε όρους χρόνου κλίμακα ζημιάς και περίοδο αποκατάστασης. Είναι σημαντικό να γίνει σύνδεση μεταξύ των διαφορετικών κινδύνων, ώστε να δημιουργηθεί μία πλήρης εικόνα των απαιτήσεων επιχειρησιακής συνέχειας του οργανισμού. Η εκτίμηση θα πρέπει να προσδιορίσει, ποσοτικοποιήσει και ιεραρχήσει τους κινδύνους σύμφωνα με τα κριτήρια και τους στόχους του

οργανισμού, συμπεριλαμβάνοντας τους κρίσιμους πόρους, τις επιπτώσεις των διακοπών, τους επιτρεπόμενους χρόνους διακοπής και της προτεραιότητες ανάκαμψης.

3. *Ανάπτυξη και εφαρμογή σχεδίων συνέχειας που θα περιλαμβάνουν την ασφάλεια ΠΣ:* η διαδικασία του σχεδιασμού θα πρέπει να εστιάζει στους επιχειρησιακούς στόχους, για παράδειγμα, η επαναφορά συγκεκριμένων υπηρεσιών επικοινωνίας και η διαθεσιμότητα της πληροφορίας θα πρέπει να επιτευχθεί εντός ενός προκαθορισμένου χρονοδιαγράμματος. Αντίγραφα των σχεδίων πρέπει να τηρούνται και σε μία απομακρυσμένη τοποθεσία, ώστε να διασωθούν σε περίπτωση καταστροφής στις κύριες εγκαταστάσεις του οργανισμού. Τα σχέδια αλλά και τα αντίγραφα αυτών πρέπει να ενημερώνονται συνεχώς και να προστατεύονται με συγκεκριμένες διαδικασίες, διότι μπορεί να περιέχουν ευαίσθητη πληροφορία.
4. *Πλαίσιο σχεδιασμού επιχειρησιακής συνέχειας:* απαραίτητο είναι ένα ενιαίο πλαίσιο επιχειρησιακής συνέχειας που θα διασφαλίζει ότι όλα τα σχέδια είναι συνεπή μεταξύ τους και ικανοποιούν τις απαιτήσεις ασφαλείας των ΠΣ. Κάθε σχέδιο θα πρέπει να περιγράφει μία προσέγγιση για συνέχεια (continuity). Επίσης, θα πρέπει να καθορίζεται ένα σχέδιο κλιμάκωσης και οι προϋποθέσεις για την ενεργοποίησή του, καθώς και τα άτομα που είναι υπεύθυνα για την εκτέλεση κάθε στοιχείου του σχεδίου. Όταν εντοπίζονται νέες απαιτήσεις, κάθε υπάρχουσα διαδικασία έκτακτης ανάγκης, θα πρέπει να τροποποιείται αναλόγως. Κάθε σχέδιο πρέπει να έχει έναν 'ιδιοκτήτη'. Οι διαδικασίες έκτακτης ανάγκης, τα εφεδρικά σχέδια και σχέδια επανέναρξης θα πρέπει να εντάσσονται στα καθήκοντα των 'ιδιοκτητών' των πόρων και διαδικασιών που εμπλέκονται.
5. *Έλεγχος, συντήρηση και αναθεώρηση σχεδίων επιχειρησιακής συνέχειας:* τα σχέδια πρέπει να ελέγχονται, συντηρούνται και ενημερώνονται σε τακτά χρονικά διαστήματα. Για να εξασφαλισθεί ότι το σχέδιο ή σχέδια θα λειτουργήσουν σε πραγματικές καταστάσεις, θα πρέπει να εφαρμοσθεί μία ποικιλία τεχνικών, όπως: α)δοκιμές διαφόρων σεναρίων επί χάρτου, β)προσομοιώσεις, γ)δοκιμές τεχνικής ανάκαμψης, δ)έλεγχοι ανάκτησης σε διαφορετικό περιβάλλον, ε)δοκιμές των εγκαταστάσεων και υπηρεσιών των προμηθευτών και στ)πλήρεις δοκιμές (δοκιμή ολόκληρου του οργανισμού, προσωπικού, εξοπλισμού, εγκαταστάσεων και διαδικασιών ότι μπορούν να αντιμετωπίσουν τις διακοπές). Τα αποτελέσματα όλων αυτών των ελέγχων θα πρέπει να καταγράφονται και να λαμβάνονται μέτρα για τη βελτίωση των σχεδίων όπου είναι απαραίτητο. Απαραίτητη είναι η κατάλληλη ενημέρωση των σχεδίων όταν εντοπίζονται αλλαγές που δεν αντικατοπτρίζονται στα σχέδια επιχειρησιακής συνέχειας, για παράδειγμα μετά την απόκτηση καινούριου εξοπλισμού, την αναβάθμιση των ΠΣ και μετά από αλλαγές στο προσωπικό, σε διευθύνσεις , σε τηλεφωνικούς αριθμούς, στη στρατηγική, σε τοποθεσίες, σε εγκαταστάσεις, σε πόρους, στη νομοθεσία, σε προμηθευτές και συνεργάτες.

2.13 Συμμόρφωση

2.13.1 Συμμόρφωση με νομοθετικό πλαίσιο

Ο σχεδιασμός, λειτουργία, χρήση και διαχείριση των ΠΣ δύναται να υπόκεινται σε συγκεκριμένες θεσμικές και κανονιστικές απαιτήσεις ασφαλείας. Συμβουλές σχετικά με το ειδικό νομοθετικό πλαίσιο που ισχύει θα πρέπει να παρέχονται από τους νομικούς συμβούλους του οργανισμού. Το νομοθετικό πλαίσιο μπορεί να διαφέρει από χώρα σε χώρα και ίσως διαφέρει για πληροφορία που δημιουργήθηκε από μία χώρα και μεταδίδεται σε μία άλλη (διασυνοριακή ροή δεδομένων).

1. *Σχετική νομοθεσία:* όλη η σχετική νομοθεσία, οι κανονισμοί και οι συμβάσεις που δεσμεύουν τον οργανισμό θα πρέπει να είναι ξεκάθαρα καθορισμένες, τεκμηριωμένες και να ενημερώνονται για το κάθε ΠΣ. Παράλληλα, θα πρέπει να ορισθούν και τεκμηριωθούν κατάλληλα τα ειδικά μέτρα ελέγχου και τα ατομικά καθήκοντα προς ικανοποίηση των παραπάνω δεσμεύσεων.
2. *Δικαιώματα πνευματικής ιδιοκτησίας:* για την προστασία κάθε υλικού που μπορεί να αποτελεί πνευματική ιδιοκτησία (λογισμικό, πηγαίος κώδικας, έγγραφα, εμπορικά σήματα, ευρεσιτεχνίες κλπ) θα πρέπει να ληφθούν ενέργειες όπως: α)δημοσίευση μίας πολιτικής συμμόρφωσης που καθορίζει τη νόμιμη χρήση του λογισμικού και των υπόλοιπων προϊόντων πληροφορικής,

β)απόκτηση λογισμικού μόνο μέσω γνωστών και αξιόπιστων πηγών, γ)ευαισθητοποίηση και επιβολή πειθαρχικών κυρώσεων στο προσωπικό που παραβιάζει τα δικαιώματα πνευματικής ιδιοκτησίας, δ)τήρηση κατάλληλου μητρώου των αγαθών, από όπου θα αποδεικνύεται η κυριότητα και εγκυρότητα όλων των αδειών χρήσης, ε)διενέργεια τακτικών ελέγχων για τη διαπίστωση ότι το εγκατεστημένο λογισμικό και προϊόντα έχουν την αντίστοιχη άδεια, στ)αποφυγή αντιγραφής εξολοκλήρου ή τμηματικά βιβλίων, άρθρων, αναφορών ή άλλων εγγράφων, εκτός αυτών επιτρέπει η νομοθεσία περί πνευματικής ιδιοκτησίας.

3. <u>*Διατήρηση αρχείων του οργανισμού:*</u> τα σημαντικά αρχεία πρέπει να προστατεύονται από την απώλεια, καταστροφή και παραποίηση, σύμφωνα με την κείμενη νομοθεσία, τους κανονισμούς και τις συμβάσεις που δεσμεύουν τον οργανισμό. Τα αρχεία πρέπει να κατηγοριοποιούνται ανάλογα με τον τύπο τους (π.χ. αρχεία διαχείρισης, αρχεία βάσεων δεδομένων, αρχεία καταγραφής συναλλαγών, ελέγχων κλπ), και με λεπτομέρειες σχετικά με την περίοδο τήρησης και το αποθηκευτικό μέσο (π.χ. χαρτί, μαγνητικά ή οπτικά μέσα). Στην περίπτωση ηλεκτρονικών μέσων αποθήκευσης, θα πρέπει να διασφαλίζεται η πρόσβαση στα δεδομένα (μέσο αποθήκευσης και μορφότυπο) καθ όλη τη διάρκεια της τήρησης, και να λαμβάνονται μέτρα προστασίας απέναντι σε απώλεια εξαιτίας μελλοντικών τεχνολογικών αλλαγών. Τα συστήματα αποθήκευσης πρέπει να εξασφαλίζουν την ανάκτηση των δεδομένων σε ένα αποδεκτό χρονοδιάγραμμα και στο σωστό μορφότυπο (format). Επιπλέον, τα συστήματα αυτά θα πρέπει να παρέχουν τη δυνατότητα καταστροφής των αρχείων μετά την υποχρεωτική περίοδο τήρησής τους και εφόσον αυτά δεν είναι απαραίτητα για τον οργανισμό. Για την επίτευξη των στόχων της ασφαλούς τήρησης των αρχείων του οργανισμού, είναι απαραίτητη μία διαδικασία η οποία θα αποτελείται από τα εξής στάδια: α)έκδοση συγκεκριμένων οδηγιών για την τήρηση, αποθήκευση, διαχείριση και διάθεση των αρχείων και της πληροφορίας, β)κατάρτιση ενός χρονοδιαγράμματος υποχρεωτικής τήρησης των αρχείων, γ)απογραφή και τήρηση των πηγών της σημαντικής πληροφορίας και δ)λήψη κατάλληλων μέτρων ελέγχου για την προστασία των αρχείων και της πληροφορίας.
4. <u>*Προστασία προσωπικών δεδομένων:*</u> είναι απαραίτητη η ύπαρξη και συμμόρφωση με μία πολιτική προστασίας προσωπικών δεδομένων, η οποία θα είναι σύμφωνη με την ισχύουσα νομοθεσία και κανονισμούς. Η καλύτερη προσέγγιση είναι συνήθως ο διορισμός ενός 'υπεύθυνου' προστασίας δεδομένων, ο οποίος θα καθοδηγεί το υπόλοιπο προσωπικό όσον αφορά τα ατομικά του καθήκοντα και τις συγκεκριμένες διαδικασίες που πρέπει να ακολουθούνται.
5. <u>*Προστασία από μη ορθή χρήση των ΠΣ:*</u> τα ΠΣ ενός οργανισμού προορίζονται κυρίως ή αποκλειστικά για επιχειρησιακούς σκοπούς. Εργαλεία παρακολούθησης, ανίχνευσης εισβολών και επιθεώρησης περιεχομένου μπορούν να συμβάλλουν στην πρόληψη και τον εντοπισμό της μη ορθής χρήσης των ΠΣ.
6. <u>*Κανόνες κρυπτογράφησης:*</u> η χρήση κρυπτογραφικών μεθόδων πρέπει να συμμορφώνεται με σχετικές οδηγίες, νόμους και κανονισμούς.

2.13.2 Συμμόρφωση με πολιτικές και πρότυπα – τεχνική συμμόρφωση

Τα ΠΣ του οργανισμού πρέπει να συμμορφώνονται με τις πολιτικές και τα πρότυπα ασφαλείας που υιοθετεί ο οργανισμός. Οι πολιτικές και τα πρότυπα θα πρέπει να αναθεωρούνται σε τακτική βάση.

1. <u>*Συμμόρφωση με πολιτικές και πρότυπα ασφαλείας:*</u> η διεύθυνση θα πρέπει να διασφαλίζει ότι πραγματοποιούνται όλες οι διαδικασίες ασφαλείας στην περιοχή αρμοδιότητάς της και πως επιτυγχάνεται συμμόρφωση με τις πολιτικές και τα πρότυπα. Σε περίπτωση μη συμμόρφωσης θα πρέπει να εντοπισθούν οι αιτίες, να εφαρμοσθούν συγκεκριμένες διορθωτικές ενέργειες, να αξιολογηθούν οι ενέργειες αυτές και τέλος, να αποφασισθούν και ληφθούν τα κατάλληλα μέτρα για την αποφυγή επανεμφάνισής της.
2. <u>*Έλεγχος τεχνικής συμμόρφωσης:*</u> ο έλεγχος τεχνικής συμμόρφωσης πρέπει να γίνεται είτε χειρωνακτικά (με την υποστήριξη κάποιου λογισμικού, εάν είναι απαραίτητο), είτε από έναν έμπειρο μηχανικό συστημάτων και με τη βοήθεια αυτοματοποιημένων εργαλείων, τα οποία να παράγουν μία τεχνική αναφορά. Εάν εκτελούνται δοκιμές ασφαλείας ή γίνονται εκτιμήσεις ευπαθειών, θα πρέπει να δίδεται ιδιαίτερη προσοχή διότι αυτές οι δραστηριότητες θα μπορούσαν να οδηγήσουν σε κενά ασφαλείας του συστήματος. Αυτά τα τεστ απεικονίζουν μία στιγμιαία

κατάσταση του συστήματος σε συγκεκριμένο χρόνο. Το στιγμιότυπο αυτό περιορίζεται στα τμήματα του συστήματος που ελέγχονται κατά τη διάρκεια της δοκιμής, γι' αυτό το λόγο τα παραπάνω τεστ δεν μπορούν να υποκαταστήσουν τη διαδικασία εκτίμησης κινδύνου.

2.13.3 Έλεγχος ασφαλείας ΠΣ

Για τη μεγιστοποίηση της αποδοτικότητας και την εξάλειψη των παρεμβολών κατά τη διαδικασία ελέγχου των ΠΣ, πρέπει να πρέπει να λαμβάνονται μέτρα για την προστασία των υπό λειτουργία ΠΣ και την ακεραιότητα των δεδομένων, αλλά και μέτρα για την αποτροπή της μη ορθής χρήσης των εργαλείων ελέγχου.

1. *Μέτρα για τον έλεγχο:* οι απαιτήσεις και οι δραστηριότητες ελέγχου που περιλαμβάνουν και υπό λειτουργία ΠΣ πρέπει να προγραμματίζονται προσεκτικά ώστε να ελαχιστοποιείται ο κίνδυνος διακοπής ή δυσχέρειας των επιχειρησιακών διαδικασιών. Θα πρέπει να ακολουθούνται τα εξής: α)καθορισμός πεδίου εφαρμογής των ελέγχων, β)μόνο-για-ανάγνωση πρόσβαση στο λογισμικό και τα δεδομένα, γ)άλλου είδους πρόσβαση θα επιτρέπεται μόνο σε απομονωμένα αντίγραφα των αρχείων συστήματος, τα οποία μετά την ολοκλήρωση του ελέγχου θα διαγράφονται, δ)οι πόροι για την εκτέλεση των ελέγχων πρέπει να αναφέρονται ρητά και να τίθενται σε διάθεση, ε)το πρόσωπο που εκτελεί τον έλεγχο θα πρέπει να είναι ανεξάρτητο από τις δραστηριότητες που ελέγχονται.
2. *Προστασία εργαλείων ελέγχου:* η πρόσβαση στα εργαλεία ελέγχου θα πρέπει να προστατεύεται από πιθανή μη ορθή χρήση ή αλλοίωση, ειδικά στη περίπτωση που στη διαδικασία συμμετέχουν και τρίτα μέρη.

3. Διαχείριση Επικινδυνότητας ΠΣ

Ο θεμελιώδης κανόνας της ασφάλειας πληροφορίας είναι η υποστήριξη της αποστολής του οργανισμού. Όλοι οι οργανισμοί είναι εκτεθειμένοι σε 'αβεβαιότητες', μερικές εκ των οποίων έχουν αρνητικές επιπτώσεις. Για την υποστήριξη του οργανισμού οι επαγγελματίες ασφάλειας ΠΣ θα πρέπει να είναι σε θέση να βοηθήσουν τη διοίκηση να κατανοήσει και να διαχειρισθεί αυτές τις 'αβεβαιότητες'. Η διαχείριση αυτή δεν είναι εύκολο έργο, διότι οι περιορισμένοι πόροι και το διαρκώς μεταβαλλόμενο τοπίο των απειλών και τρωτοτήτων καθιστούν τον εξολοκλήρου περιορισμό των κινδύνων αδύνατο. Ως εκ τούτου οι επαγγελματίες ασφαλείας ΠΣ θα πρέπει να διαθέτουν ένα σύνολο εργαλείων που θα τους βοηθά να μοιράζονται μία κοινή άποψη με τη διοίκηση αναφορικά με τις πιθανές επιπτώσεις των απειλών που σχετίζονται με τα ΠΣ, και το οποίο θα πρέπει να είναι σταθερό, επαναλαμβανόμενο, οικονομικό και να μειώνει τους κινδύνους σε ένα αποδεκτό επίπεδο [22].

Κίνδυνος είναι η πιθανή βλάβη που μπορεί να προκύψει από μία τρέχουσα διαδικασία ή ένα μελλοντικό γεγονός. Η διαχείριση επικινδυνότητας είναι η διαδικασία κατανόησης και αντιμετώπισης των παραγόντων που μπορεί να οδηγήσουν σε μία αποτυχία εμπιστευτικότητας, ακεραιότητας ή διαθεσιμότητας ενός ΠΣ. Κίνδυνος ασφαλείας ΠΣ είναι η βλάβη σε μία διαδικασία ή στη σχετική πληροφορία ως αποτέλεσμα ενός σκόπιμου ή ατυχηματικού γεγονότος το οποίο έχει αρνητικές επιπτώσεις σε αυτές.

Κίνδυνος *είναι η συνάρτηση της πιθανότητας μίας συγκεκριμένης* ***πηγής-απειλής*** *να εκμεταλλευθεί μία συγκεκριμένη* ***ευπάθεια*** *και της* ***επίπτωσης*** *αυτού του ανεπιθύμητου συμβάντος στον οργανισμό.(NIST SP-800-30).*

Απειλή *είναι η δυνατότητα μια πηγή-απειλή να εκμεταλλευθεί (κατά λάθος ή σκοπίμως) μία συγκεκριμένη ευπάθεια (NIST SP-800-30).*

Πηγή-απειλής *είναι είτε (1) η με πρόθεση και μεθοδικά στοχευμένη εκμετάλλευση μίας ευπάθειας είτε (2) μία κατάσταση που μπορεί να προκαλέσει τυχαία μία ευπάθεια (NIST SP-800-30).*

Η απειλή είναι απλά η δυνατότητα εκμετάλλευσης μίας συγκεκριμένης ευπάθειας. Οι απειλές από μόνες τους δεν αποτελούν ενέργειες. Θα πρέπει να συνδυαστούν με κάποια πηγή-απειλής ώστε να γίνουν επικίνδυνες. Πρόκειται για μία σημαντική διάκριση κατά την αξιολόγηση και διαχείριση των κινδύνων, δεδομένου ότι κάθε πηγή-απειλής μπορεί να έχει διαφορετική πιθανότητα εμφάνισης, επηρεάζοντας την εκτίμηση και διαχείριση κινδύνων. Είναι χρήσιμο να ενσωματώνονται οι πηγές με τις απειλές. Ο παρακάτω πίνακας παρουσιάζει ορισμένες από τις πιθανές απειλές των ΠΣ λαμβάνοντας υπόψη τις πηγές-απειλών:

Απειλή (συμπεριλαμβανομένης της πηγής-απειλής)	**Περιγραφή**
Ατυχηματική αποκάλυψη	Η μη εξουσιοδοτημένη ή ατυχηματική αποκάλυψη της διαβαθμισμένης, προσωπικής ή ευαίσθητης πληροφορίας
Φυσικά φαινόμενα	Όλα τα είδη φυσικών φαινομένων (σεισμοί, τυφώνες, ανεμοστρόβιλοι) που μπορούν να βλάψουν ή επηρεάσουν το ΠΣ ή την εφαρμογή. Οποιαδήποτε από αυτές τις πιθανές απειλές μπορούν να οδηγήσουν σε μερική ή ολική διακοπής, επηρεάζοντας με αυτό τον τρόπο τη διαθεσιμότητα.
Μεταβολή λογισμικού	Οποιαδήποτε με πρόθεση τροποποίηση, προσθήκη, διαγραφή του λειτουργικού συστήματος ή εφαρμογών, είτε από εξουσιοδοτημένο χρήστη είτε όχι, και η οποία θέτει σε κίνδυνο την εμπιστευτικότητα, διαθεσιμότητα ή ακεραιότητα των δεδομένων, του συστήματος ή των πόρων που ελέγχονται από το ΠΣ.
Εύρος ζώνης	Η τυχαία ή σκόπιμη χρήση του εύρους ζώνης των επικοινωνιών για άλλους σκοπούς.
Ηλεκτρικές παρεμβολές/διακοπές	Οποιαδήποτε παρεμβολή ή διακύμανση που μπορεί να προκύψει ως αποτέλεσμα μίας διακοπής ρεύματος. Αυτό μπορεί να

	προκαλέσει άρνηση παροχής υπηρεσιών σε εξουσιοδοτημένους χρήστες (αποτυχία) ή τροποποίηση δεδομένων (διακύμανση).
Σκόπιμη αλλοίωση δεδομένων	Οποιαδήποτε με πρόθεση τροποποίηση, εισαγωγή ή διαγραφή δεδομένων, η οποία διακυβεύει την εμπιστευτικότητα, διαθεσιμότητα ή ακεραιότητα των δεδομένων που παράγονται, επεξεργάζονται, ελέγχονται ή αποθηκεύονται από συστήματα επεξεργασίας δεδομένων.
Σφάλμα διαμόρφωσης συστήματος (τυχαίο)	Οποιοδήποτε τυχαίο σφάλμα διαμόρφωσης κατά την αρχική εγκατάσταση ή αναβάθμιση υλικού, λογισμικού, εξοπλισμού επικοινωνίας κλπ.
Βλάβη/Διακοπή τηλεπικοινωνιών	Οποιαδήποτε βλάβη σύνδεσης ή μονάδας επικοινωνίας ικανή να προκαλέσει διακοπή στη μετάδοση δεδομένων διαμέσου τηλεπικοινωνιών μεταξύ τερματικών υπολογιστών απομακρυσμένων ή κατανεμημένων επεξεργαστών και εγκαταστάσεις φιλοξενίας (hosting).

Πίνακας 1. Περιγραφή απειλών

Ευπάθεια (ή αδυναμία) *είναι ένα ελάττωμα ή μία αδυναμία στις διαδικασίες ασφαλείας, το σχεδιασμό, την υλοποίηση του ΠΣ ή στην εκτέλεση εσωτερικών ελέγχων και που έχουν ως αποτέλεσμα να δημιουργηθεί κενό ασφαλείας ή να παραβιασθεί η πολιτική ασφαλείας(NIST SP-800-30).*

Ο κυριότερος λόγος της διαχείρισης κινδύνων μέσα σε ένα οργανισμό είναι η προστασία της αποστολής και των αγαθών του. Γι' αυτό ακριβώς το λόγο η διαχείριση κινδύνων θα πρέπει να είναι μία λειτουργία διοίκησης παρά μία τεχνική λειτουργία. Η διαχείριση κινδύνων είναι ζωτικής σημασίας για τα ΠΣ. Η κατανόησή των συγκεκριμένων κινδύνων ενός ΠΣ επιτρέπουν στον 'ιδιοκτήτη' του να λάβει τα απαραίτητα μέτρα προστασίας ανάλογα με την αξία που έχει για τον οργανισμό. Λόγω των περιορισμένων πόρων που διαθέτουν οι οργανισμοί, οι κίνδυνοι είναι αδύνατο να μηδενιστούν. Έτσι, η κατανόησή του μεγέθους των κινδύνων, επιτρέπουν σε ένα οργανισμό να δέσει προτεραιότητα στη διάθεση των πόρων.

3.1 Ανάλυση κινδύνου

Η ανάλυση του κινδύνου γίνεται μέσα από τον εντοπισμό των απειλών και ευπαθειών του ΠΣ, τον καθορισμό της πιθανότητας εμφάνισης και των επιπτώσεων που θα έχει ο κάθε κίνδυνος. Πρόκειται για μία περίπλοκη διαδικασία η οποία συνήθως βασίζεται σε ελλιπείς πληροφορίες. Υπάρχουν διάφορες μεθοδολογίες για την ανάλυση κινδύνου οι οποίες είναι επαναλαμβανόμενες και παρέχουν συνεπή αποτελέσματα. Γενικά όμως υπάρχουν δύο μεγάλες κατηγορίες: 1) η ποσοτική και 2) η ποιοτική ανάλυση [22].

3.1.1 Ποσοτική Ανάλυση Κινδύνου (Quantitative Risk Assessment)

Η ποσοτική ανάλυση κινδύνου στηρίζεται σε μεθοδολογίες που χρησιμοποιούνται από χρηματοπιστωτικά ιδρύματα και ασφαλιστικές εταιρίες. Γίνεται 'ποσοτικοποίηση' όλων των σταθερών (αξία πληροφορίας, συστημάτων, επιχειρησιακών διαδικασιών, κόστη ανάκτησης κλπ) με αποτέλεσμα να υπολογίζεται ο αντίκτυπος και κατ' επέκταση ο κίνδυνος με όρους άμεσων και έμμεσων δαπανών. Μαθηματικά, η ποσοτική ανάλυση μπορεί να εκφραστεί από το Εκτιμώμενο Ετήσιο Κόστος-ΕΕΚ (Annualized Loss Expectancy-ALE) [22]. Το ΕΕΚ είναι η αναμενόμενη χρηματική απώλεια για ένα αγαθό σε σχέση με τον κίνδυνο που εμφανίζονται σε περίοδο ενός έτους.

ΕΕΚ=ΠΜΑ*ΕΡΕ

Όπου:

- **ΠΜΑ**: Προσδοκία Μεμονωμένης Απώλειας (Single Loss Expectancy-SLE) είναι η αξία μίας μεμονωμένης απώλειας αγαθού και αντίκτυπος που θα έχει η απώλεια αυτή στο ΠΣ.
- **ΕΡΕ**: Ετήσιος Ρυθμός Εμφάνισης (Annualized Rate of Occurrence) είναι η συχνότητα που μία απώλεια συμβαίνει. Είναι η πιθανότητα εμφάνισης της απώλειας.

Η ποσοτική ανάλυση φαινομενικά είναι απλή και λογική, στην πράξη όμως προκύπτουν ζητήματα όταν αυτή εφαρμόζεται στα ΠΣ. Καθώς το κόστος ενός ΠΣ μπορεί να είναι εύκολο να προσδιορισθεί, η αξία της πληροφορίας, της απώλειας μίας παραγωγικής διαδικασίας και το κόστος ανάκτησης δεν είναι δυνατό να καθορισθεί. Περαιτέρω, το άλλο σημαντικό στοιχείο του κινδύνου, η πιθανότητα εμφάνισής του, είναι ακόμη λιγότερο γνωστή. Για παράδειγμα, ποια είναι η πιθανότητα κάποιος να χρησιμοποιήσει την κοινωνική δικτύωση για να αποκτήσει πρόσβαση σε ένα λογαριασμό χρήστη σε ένα ΠΣ;

Ως εκ τούτου, υπάρχει ένα μεγάλο περιθώριο σφάλματος που είναι συνυφασμένο με την ποσοτική ανάλυση κινδύνου στα ΠΣ. Βέβαια, με τη χρήση διαθέσιμων στατιστικών στοιχείων είναι δυνατή η εκμετάλλευση της εμπειρίας του παρελθόντος. Οι ασφαλιστικές εταιρίες και τα χρηματοπιστωτικά ιδρύματα χρησιμοποιούν εξαιρετικά τα στατιστικά στοιχεία για να εξασφαλίζουν ότι οι ποσοτικές αναλύσεις τους είναι ουσιαστικές, επαναλαμβανόμενες και συνεπείς. Συνήθως η εκτέλεση ποσοτικής ανάλυσης κινδύνου στα ΠΣ δεν είναι αποδοτική κι αυτό λόγω της σχετικής δυσκολίας απόκτησης ακριβής και πλήρης πληροφορίας. Ωστόσο, εάν η πληροφορία είναι αξιόπιστη, η ποσοτική ανάλυση είναι ένα εξαιρετικά χρήσιμο εργαλείο για την κοινοποίηση του κινδύνου σε όλα τα επίπεδα της διοίκησης.

Η ποσοτική μέτρηση του κινδύνου είναι ο συνήθης τρόπος μέτρησης σε πολλούς τομείς, όπως στην ασφάλιση, αλλά δεν είναι η συνήθης μέθοδος στα ΠΣ. Αυτό συμβαίνει για τους εξής δύο λόγους: 1) οι δυσκολίες εντοπισμού και απόδοσης αξιών στα αγαθά και 2) την έλλειψη στατιστικής πληροφορίας η οποία να καθιστά εφικτό τον προσδιορισμό της συχνότητας εμφάνισης μίας απώλειας. Για τους παραπάνω λόγους τα περισσότερα εργαλεία ανάλυσης κινδύνου που χρησιμοποιούνται σήμερα στα ΠΣ βασίζονται στην ποιοτική μέτρηση της επικινδυνότητας, η οποία παρουσιάζεται στη συνέχεια.

3.2.1 Ποιοτική Ανάλυση Κινδύνου (Qualitative Risk Assessment)

Οι ποιοτικές αναλύσεις κινδύνου βασίζονται στην εξαρχής υπόθεση ότι υπάρχει ένας μεγάλος βαθμός αβεβαιότητας στην πιθανότητα εμφάνισης και την αξία της επίπτωσης, με συνέπεια ο ορισμός του κινδύνου να γίνεται με έναν τρόπο υποκειμενικό, χρησιμοποιώντας ποιοτικούς όρους. Η μεγάλη δυσκολία στην ποιοτική ανάλυση, όπως άλλωστε και στην ποσοτική, είναι ο ορισμός της πιθανότητας εμφάνισης και της αξίας των επιπτώσεων. Αυτές οι τιμές θα πρέπει να ορισθούν με τέτοιο τρόπο που να επιτρέπει τη χρησιμοποίηση των ίδιων μεγεθών σε πολλαπλές αναλύσεις. Τα αποτελέσματα των ποιοτικών αναλύσεων είναι εκ φύσεως πιο δύσκολο να διοχετευθούν στη διοίκηση. Συνήθως τα αποτελέσματα που δίνουν είναι τιμές όπως 'ΥΨΗΛΗ', 'ΜΕΤΡΙΑ, 'ΧΑΜΗΛΗ'. Ωστόσο, με κατάλληλους πίνακες ορισμού της πιθανότητας εμφάνισης και με τη σωστή περιγραφή των επιπτώσεων, η ενημέρωση της διοίκησης σχετικά με την επικινδυνότητα μπορεί να είναι επαρκής [22].

Εντοπισμός απειλών

Για την εξασφάλιση ακριβής ανάλυσης θα πρέπει να καθορίζονται τόσο οι απειλές όσο και οι πηγές τους. Ορισμένες από τις πιο συχνές πηγές απειλών είναι οι φυσικές απειλές (πλημμύρες, σεισμοί κλπ), οι ανθρώπινες απειλές (χωρίς πρόθεση ή εσκεμμένες ενέργειες) και οι απειλές περιβάλλοντος (διακοπή ρεύματος, ρύπανση, χημικές ουσίες κλπ). Το κλειδί στον εντοπισμό των απειλών είναι τα άτομα που έχουν γνώση της λειτουργίας του οργανισμού ή του τύπου του ΠΣ (ή ακόμα καλύτερα και στα δύο). Σημαντική είναι η δημιουργία ενός καταλόγου των απειλών που αντιμετωπίζει ολόκληρος ο οργανισμός, ο οποίος θα χρησιμοποιηθεί ως βάση για όλες τις δραστηριότητες διαχείρισης επικινδυνότητας.

Εντοπισμός ευπαθειών (αδυναμιών)

Ο εντοπισμός των ευπαθειών μπορεί να γίνει με διάφορα μέσα. Διαφορετικά σχήματα διαχείρισης επικινδυνότητας προσφέρουν και διαφορετικές μεθοδολογίες. Αρχικά, χρησιμοποιούνται οι πιο κοινοί κατάλογοι ευπαθειών ή σημείων ελέγχου. Στη συνέχεια, και σε συνεργασία με τους 'ιδιοκτήτες' συστημάτων ή άλλα άτομα με γνώσεις πάνω στο ΠΣ και στον οργανισμό γενικότερα, εντοπίζονται συγκεκριμένα οι ευπάθειες του ΠΣ. Ο εντοπισμός μπορεί να γίνει και μέσα από έρευνα σε ιστοσελίδες προμηθευτών ή δημόσιους καταλόγους, όπως η βάση δεδομένων με τις Συνήθεις Ευπάθειες και Τρωτότητες (Common Vulnerabilities and Exposures-CVE-)[1] και η Εθνική Βάση Ευπαθειών (National Vulnerability Database-NVD-)[2], έτσι ώστε σε περίπτωση που υπάρχουν υφιστάμενες αναλύσεις επικινδυνότητας και αναφορές ελέγχων, να χρησιμοποιηθούν ως βάση.

Επιπρόσθετα, παρόλο που τα παρακάτω εργαλεία και τεχνικές συνήθως χρησιμοποιούνται για την αξιολόγηση της αποδοτικότητας των μέτρων ελέγχου, μπορούν παράλληλα να χρησιμοποιηθούν και για τον εντοπισμό ευπαθειών:

- Σαρωτές ευπαθειών: λογισμικό που εξετάζει ένα λειτουργικό σύστημα, μία δικτυακή εφαρμογή ή τμήματα κώδικα συγκρίνοντας το ΠΣ (ή την απόκριση του συστήματος) με μία βάση ελαττωμάτων.
- Δοκιμές: προσπάθεια αναλυτών ασφαλείας να εξαπολύουν απειλές ενάντια στο ΠΣ, π.χ. μέσα από την κοινωνική δικτύωση.
- Έλεγχος των μέτρων ελέγχου: εμπεριστατωμένη αναθεώρηση των μέτρων ελέγχου λειτουργίας και διαχείρισης μέσα από τη σύγκριση με βέλτιστες πρακτικές (για παράδειγμα το Διεθνές Πρότυπο ISO/IEC 27002) , καθώς και μέσα από τη σύγκριση των πραγματικών πρακτικών με τις τρέχουσες τεκμηριωμένες διαδικασίες.

Συσχέτιση Απειλών - Ευπαθειών (Α-Ε)

Ένα από τα πιο δύσκολα σημεία της διαχείρισης επικινδυνότητας είναι η συσχέτιση μίας απειλής με μία ευπάθεια. Ωστόσο, η δημιουργία αυτής της συσχέτισης είναι απαραίτητη, μιας και ο κίνδυνος ορίζεται ως η άσκηση μίας απειλής σε βάρος μίας ευπάθειας. Είναι λογικό ότι κάθε απειλή (ενέργεια) δεν μπορεί να ασκηθεί ενάντια σε κάθε ευπάθεια. Για παράδειγμα, η απειλή 'πλημμύρα' προφανώς ισχύει για μία ευπάθεια όπως η έλλειψη σχεδίου έκτακτης ανάγκης και όχι στην αποτυχία αλλαγής των προεπιλεγμένων ελεγκτών αυθεντικοποίησης. Αν και φαίνεται λογική η ύπαρξη και χρησιμοποίηση ενός πρότυπου συνόλου Α-Ε, στην πραγματικότητα δεν υπάρχει κάτι αντίστοιχο που να είναι άμεσα διαθέσιμο. Αυτό μπορεί να οφείλεται στο γεγονός ότι συνεχώς εντοπίζονται νέες απειλές με αποτέλεσμα η συσχέτιση Α-Ε να αλλάζει διαρκώς. Παρόλα αυτά θα πρέπει να αναπτυχθεί και να λειτουργήσει ως βάση μία τυποποιημένη λίστα αντιστοίχισης Α-Ε μέσα σε ένα οργανισμό. Η ανάπτυξη αυτής της λίστας μπορεί να επιτευχθεί μέσα τη συνεχή αξιολόγηση των ευπαθειών και αντιστοίχιση τους με κάθε απειλή που μπορεί να υπάρξει. Αυτή η τυποποιημένη λίστα θα πρέπει να προσαρμοστεί σε κάθε σύστημα.

Ορισμός Πιθανότητας Εμφάνισης (Likelihood)

Ο ορισμός της πιθανότητας εμφάνισης είναι αρκετά απλός. Πρόκειται για την πιθανότητα εμφάνισης μίας απειλής σε σχέση με μία ευπάθεια. Η χρησιμοποίηση ενός τυποποιημένου ορισμού της πιθανότητας εμφάνισης για όλες τις αναλύσεις επικινδυνότητας, διασφαλίζει τη συνέπεια. Σε κάθε περίπτωση θα πρέπει να δοθεί ιδιαίτερη προσοχή σε αυτούς τους ορισμούς. Στον ορισμό που φαίνεται στον παρακάτω πίνακα προκύπτει μία κωδωνοειδής καμπύλη (η μέτρια πιθανότητα έχει διπλάσιο ποσοστό από ότι μία χαμηλή ή μία υψηλή). Από κάποιον άλλο ορισμό μπορεί να προκύπτει μία ευθεία καμπύλη (Χαμηλή:0-33%, Μέτρια:34-76%, Υψηλή:77-100%) ή να ορίζονται παραπάνω επίπεδα (π.χ. Πολύ Χαμηλή, Χαμηλή, Μέτρια, Υψηλή, Πολύ Υψηλή). Το πιο σημαντικό πράγμα σε τελική ανάλυση είναι να διασφαλίζεται ότι οι ορισμοί χρησιμοποιούνται με συνέπεια και είναι ξεκάθαροι και κατανοητοί τόσο στη διοίκηση όσο και στην ομάδα που κάνει την ανάλυση επικινδυνότητας.

[1] http://cve.mitre.gov
[2] http://nvd.nist.gov

	Ορισμός
Χαμηλή	0-25% πιθανότητα να συμβεί με επιτυχία μία απειλή σε ετήσια περίοδο
Μέτρια	26-75% πιθανότητα να συμβεί με επιτυχία μία απειλή σε ετήσια περίοδο
Υψηλή	76-100% πιθανότητα να συμβεί με επιτυχία μία απειλή σε ετήσια περίοδο

Πίνακας 2. Πιθανότητα εμφάνισηςαπειλής

Αποτίμηση Επιπτώσεων

Για τη διασφάλιση της επαναληψιμότητας (repeatability) των αποτελεσμάτων η αποτίμηση των επιπτώσεων θα πρέπει να γίνεται με βάση τη διαθεσιμότητα, ακεραιότητα και εμπιστευτικότητα. Στον πίνακα απεικονίζεται μία λειτουργική προσέγγιση για την αποτίμηση των επιπτώσεων, εστιάζοντας σε τρεις πτυχές της ασφάλειας ΠΣ. Ωστόσο, για να έχει νόημα η διαδικασία αυτή, να είναι επαναχρησιμοποιήσιμη και να μπορεί να μεταφερθεί σε όλα τα επίπεδα της διοίκησης, θα πρέπει να παράγονται ειδικές αποτιμήσεις για ολόκληρο τον οργανισμό. Ο πίνακας παρουσιάζει αυτές τις ειδικές αποτιμήσεις.

	Εμπιστευτικότητα	Ακεραιότητα	Διαθεσιμότητα
Χαμηλή	Απώλεια εμπιστευτικότητας που οδηγεί σε **περιορισμένες** επιπτώσεις στον οργανισμό	Απώλεια ακεραιότητας που οδηγεί σε **περιορισμένες** επιπτώσεις στον οργανισμό	Απώλεια διαθεσιμότητας που οδηγεί σε **περιορισμένες** επιπτώσεις στον οργανισμό
Μέτρια	Απώλεια εμπιστευτικότητας που οδηγεί σε **σοβαρές** επιπτώσεις στον οργανισμό	Απώλεια ακεραιότητας που οδηγεί σε **σοβαρές** επιπτώσεις στον οργανισμό	Απώλεια διαθεσιμότητας που οδηγεί σε **σοβαρές** επιπτώσεις στον οργανισμό
Υψηλή	Απώλεια εμπιστευτικότητας που οδηγεί σε **ανεπανόρθωτες** επιπτώσεις στον οργανισμό	Απώλεια ακεραιότητας που οδηγεί σε **ανεπανόρθωτες** επιπτώσεις στον οργανισμό	Απώλεια διαθεσιμότητας που οδηγεί σε **ανεπανόρθωτες** επιπτώσεις στον οργανισμό

Πίνακας 3. Αποτίμηση Επιπτώσεων

Τύπος επίπτωσης	Επίπτωση στην ικανότητα εκτέλεσης αποστολής του οργανισμού	Οικονομική απώλεια/ απώλεια αγαθών	Επίπτωση στην ανθρώπινη ζωή
Περιορισμένη	Προσωρινή απώλεια μίας ή περισσότερων δευτερευόντων αποστολών	<5,000€	Ελαφριά βλάβη (κοψίματα, εκδορές κλπ)
Σοβαρή	Μεγάλης διάρκειας απώλεια μίας ή περισσότερων δευτερευόντων ή προσωρινή απώλεια μίας ή περισσότερων πρωταρχικών αποστολών	5,000-100,000€	Σημαντική βλάβη, <u>όχι</u> απειλή ανθρώπινης ζωής
Ανεπανόρθωτη	Μεγάλης διάρκειας απώλεια μίας ή περισσότερων πρωταρχικών αποστολών	>100,000€	Απώλεια ανθρώπινης ζωής ή σοβαρός τραυματισμός που θέτει σε κίνδυνο την ανθρώπινη ζωή

Πίνακας 4. Χαρακτηρισμός επιπτώσεις

Εκτίμηση κινδύνου

Η εκτίμηση κινδύνου είναι η διαδικασία προσδιορισμού της πιθανότητας να συμβεί μία απειλή σε σχέση με μία ευπάθεια και ο προσδιορισμός των επιπτώσεων μίας επιτυχούς διεκπεραίωσης. Κατά την εκτίμηση της πιθανότητας και της επίπτωσης, πρέπει να λαμβάνεται υπόψη το τρέχον περιβάλλον

απειλών. Η εκτίμηση πρέπει να γίνεται κατά τη διάρκεια λειτουργίας του ΠΣ και δεν πρέπει να λαμβάνονται υπόψη άλλα προγραμματισμένα μέτρα ελέγχου. Ο παρακάτω πίνακας χρησιμοποιεί ένα σύστημα αξιολόγησης τριών επιπέδων για την αξιολόγηση του κινδύνου. Η εκτίμηση κινδύνου καλό είναι να μη χρησιμοποιεί αριθμητικές τιμές.

Ο λόγος της αποφυγής παροχής μεγαλύτερης λεπτομέρειας στην έκθεση αξιολόγησης από αυτή που ήταν διαθέσιμη κατά τη διαδικασία της ανάλυσης είναι ανάλογος με τη χρησιμοποίηση των σημαντικών ψηφίων στη φυσική. Σε γενικές γραμμές, σημαντικά είναι τα ψηφία που σε μία μέτρηση είναι αξιόπιστα. Ως εκ τούτου είναι αδύνατο να επιτευχθεί μεγαλύτερη ακρίβεια στο αποτέλεσμα από αυτή που ήταν διαθέσιμη από την πηγή δεδομένων. Υπό αυτή την έννοια, αφού η πιθανότητα και οι επιπτώσεις αξιολογήθηκαν στη βάση Χαμηλό, Μέτριο, Υψηλό, στην ίδια βάση θα πρέπει να αξιολογηθεί και ο κίνδυνος.

Εάν η έκθεση αξιολόγησης κινδύνων δεν επιτυγχάνει το επιθυμητό επίπεδο αναλυτικότητας, θα πρέπει να αυξηθούν τα επίπεδα αξιολόγησης της πιθανότητας εμφάνισης και επίπτωσης. Σε ορισμένους οργανισμούς προτιμάται η χρήση τεσσάρων ή και πέντε επιπέδων. Σε αυτή την περίπτωση, τα επιμέρους επίπεδα θα πρέπει να ορίζονται περιληπτικά.

		Επίπτωση		
		Υψηλή	**Μέτρια**	**Χαμηλή**
Πιθανότητα εμφάνισης	**Υψηλή**	Υψηλός	Υψηλός	Μέτριος
	Μέτρια	Υψηλός	Μέτριος	Χαμηλός
	Χαμηλή	Μέτριος	Χαμηλός	Χαμηλός

Πίνακας 5. Πίνακας εκτίμησης κινδύνου τριών (3) επιπέδων

3.2 Διαχείριση κινδύνου

Η ανάλυση κινδύνου έχει ως στόχο την υποβοήθηση της διοίκησης για τον καθορισμό της διάθεσης των πόρων. Υπάρχουν τέσσερις (4) στρατηγικές για τη διαχείριση του κινδύνου: η **άμβλυνση (mitigation)**, η **μεταφορά (transference)**, η **αποδοχή (acceptance)** και η **αποφυγή (avoidance)**, οι οποίες θα αναλυθούν στη συνέχεια. Για κάθε κίνδυνο στην έκθεση αξιολόγησης, θα πρέπει να σχεδιάζεται μία στρατηγική διαχείρισής του, που θα τον μειώνει σε ένα αποδεκτό επίπεδο με ένα αποδεκτό κόστος. Επίσης, θα πρέπει να καθορίζεται το κόστος και τα βασικά στάδια υλοποίησης της στρατηγικής, γνωστό ως Σχέδιο Δράσης και Σημείων Αναφοράς (Plan of Action & Milestones-POA&M) [22].

3.2.1 Στρατηγικές διαχείρισης κινδύνου

Άμβλυνση Κινδύνου (mitigation)

Πρόκειται για την πιο συνήθη στρατηγική διαχείρισης κινδύνου, η οποία περιλαμβάνει την επιδιόρθωση κάθε ατέλειας του ΠΣ ή την παροχή κάποιου είδους αντισταθμιστικών μέτρων ελέγχου για τη μείωση της πιθανότητας εμφάνισης ή των επιπτώσεων που σχετίζονται με τη συγκεκριμένη ατέλεια. Μία κοινή πρακτική άμβλυνσης μίας ατέλειας που αφορά σε κάποιο τεχνικό θέμα ασφάλειας είναι η εγκατάσταση ενημερωμένου τμήματος κώδικα (patch) από τον προμηθευτή. Η διαδικασία καθορισμού της συγκεκριμένης στρατηγικής συχνά αναφέρεται και ως ανάλυση ελέγχου.

Μεταφορά Κινδύνου (transference)

Πρόκειται για μία διαδικασία που επιτρέπει σε κάποιο τρίτο να αποδεχτεί τον κίνδυνο για λογαριασμό του οργανισμού. Η στρατηγική αυτή δεν είναι ευρέως διαδεδομένη στα ΠΣ, αλλά συμβαίνει κατά κόρον σε άλλους τομείς, όπως της υγείας, των μεταφορών κλπ. Σε αυτές τις περιπτώσεις ο κίνδυνος μεταφέρεται σε έναν ασφαλιστή. Η στρατηγική αυτή δε μειώνει την πιθανότητα εμφάνισης ούτε επιδιορθώνει κάποια ατέλεια, αλλά στόχο έχει τη μείωση των επιπτώσεων στον οργανισμό (κυρίως των οικονομικών επιπτώσεων).

Αποδοχή Κινδύνου (Acceptance)

Πρόκειται για μία πρακτική που επιτρέπει τη λειτουργία του ΠΣ αποδεχόμενη έναν υφιστάμενο κίνδυνο. Αρκετοί κίνδυνοι που έχουν χαρακτηρισθεί χαμηλού επιπέδου, αλλά και κίνδυνοι που έχουν πολύ υψηλό κόστος αντιμετώπισης απλά γίνονται αποδεκτοί. Η συγκεκριμένη στρατηγική θα πρέπει σε κάθε περίπτωση να γίνει αποδεκτή από τα στελέχη που λαμβάνουν τις αποφάσεις. Είναι πολύ συχνό το φαινόμενο να γίνονται αποδεκτοί κίνδυνοι που δε θα έπρεπε, και εν συνεχεία όταν συμβαίνουν θεωρούνται υπεύθυνο το προσωπικό ασφαλείας ΠΣ. Η αποδοχή ή όχι ενός κινδύνου είναι απόφαση της διοίκησης και όχι του προσωπικού ασφαλείας.

Αποφυγή Κινδύνου (Avoidance)

Πρόκειται για μία πρακτική απομάκρυνσης των ευπαθειών του ΠΣ ή ακόμα και του ίδιου του ΠΣ. Για παράδειγμα, κατά τη διάρκεια της ανάλυσης, εντοπίζεται μία ιστοσελίδα που επιτρέπει στους προμηθευτές να έχουν πρόσβαση στα τιμολόγιά τους, χρησιμοποιώντας ένα αναγνωριστικό χρήστη ενσωματωμένο στο αρχείο HTML για την ταυτοποίησή τους χωρίς να γίνεται αυθεντικοποίηση ή εξουσιοδότηση. Η απόφαση της διοίκησης θα μπορούσε να είναι αφαίρεση των ιστοσελίδων και παροχή των τιμολογίων στους προμηθευτές με άλλο μηχανισμό. Σε αυτή την περίπτωση ο κίνδυνος απεφεύχθη με την απομάκρυνση των ευάλωτων ιστοσελίδων.

3.2.2 Γνωστοποίηση Κινδύνων και Στρατηγικών Διαχείρισης

Από τη στιγμή που θα ολοκληρωθεί η ανάλυση κινδύνου, τα αποτελέσματα και οι στρατηγικές διαχείρισης θα πρέπει να γίνονται γνωστά στη διοίκηση του οργανισμού και με όρους κατανοητούς, μιας και τα ανώτερα στελέχη δεν έχουν εξειδικευμένες τεχνικές γνώσεις. Στην ποσοτική ανάλυση, οι τελικές αποφάσεις βασίζονται συνήθως στην σύγκριση του κόστους κινδύνου και στο κόστος υλοποίησης της στρατηγικής διαχείρισής του. Η έκθεση αξιολόγησης θα πρέπει να περιλαμβάνει και μία ανάλυση ανταποδοτικού οφέλους (return on investment-ROI) της επένδυσης. Πρόκειται για ένα εργαλείο που χρησιμοποιείται στις επιχειρήσεις κατά κόρον για την τεκμηρίωση λήψης ή όχι μίας συγκεκριμένης δράσης, και με το οποίο η διοίκηση είναι πολύ εξοικειωμένη για τη λήψη αποφάσεων.

Στην ποιοτική ανάλυση η γνωστοποίηση είναι πιο δύσκολη διαδικασία. Καθότι το κόστος των στρατηγικών διαχείρισης είναι συνήθως γνωστό, το κόστος της μη υλοποίησής τους δεν είναι, μιας και αυτός είναι ο λόγος που επιλέχθηκε η συγκεκριμένη ανάλυση. Σε αυτή την περίπτωση μία περιγραφή *«φιλική προς τη διοίκηση»* των επιπτώσεων και της πιθανότητας εμφάνισης κάθε κινδύνου και της στρατηγικής διαχείρισης μπορεί να αποδειχθεί πολύ αποτελεσματική, και παράλληλα, μία παρουσίαση του εναπομείναντος κινδύνου ύστερα από την υλοποίηση της στρατηγικής θα αιτιολογούσε την ψήφιση των προτεινόμενων μέτρων από τη διοίκηση.

3.2.3 Υλοποίηση στρατηγικών διαχείρισης κινδύνου

Η έκθεση αξιολόγησης κινδύνων η οποία πρόκειται να παρουσιασθεί στη διοίκηση θα πρέπει να περιλαμβάνει ένα Σχέδιο Δράσης και Σημείων Αναφοράς (Plan of Action & Milestones-POAM). Πρόκειται για ένα εργαλείο με το οποίο γνωστοποιείται στη διοίκηση το προτεινόμενο χρονοδιάγραμμα και αυτό που συμβαίνει στην πραγματικότητα της υλοποίησης των στρατηγικών διαχείρισης κινδύνου. Το πρώτο βήμα της υλοποίησης είναι η καταρχήν έγκριση από τη διοίκηση του Σχεδίου [22]. Εν συνεχεία, οι ομάδες εργασίας και οι υπεύθυνοι του κάθε έργου αναφέρουν την πρόοδό τους στη διοίκηση, η οποία με τη σειρά της εποπτεύει όλη την εν εξελίξει διαδικασία της διαχείρισης κινδύνου.

Στον παρακάτω πίνακα παρουσιάζεται ένα τυπικό Σχέδιο Δράσης και Σημείων Αναφοράς [4] [12]. Σε αυτό τον πίνακα (που βασίζεται στα [4] [12]) περιλαμβάνονται τα εξής στοιχεία:

Στήλη Α-Αναγνωριστικό (ID): ένα μοναδικό αναγνωριστικό πρέπει να ανατεθεί σε κάθε στοιχείο του Σχεδίου.

Στήλη Β – Περιγραφή Ευπάθειας: μία περιγραφή των κινδύνων που εντοπίστηκαν στη διαδικασία της αξιολόγησης. Ευαίσθητες περιγραφές συγκεκριμένων ευπαθειών δεν είναι απαραίτητες, αλλά θα πρέπει να παρέχονται επαρκή στοιχεία ώστε να είναι δυνατή η επόπτευση, παρακολούθηση και να υπάρχει καλή γνώση της αδυναμίας ώστε να διευκολύνεται η δημιουργία συγκεκριμένων σημείων αναφοράς για την αντιμετώπιση του κινδύνου.

Στήλη Γ – Σημείο Επαφής (Point of Contact-POC): Προσδιορισμός ενός προσώπου/ρόλου το οποίο θα είναι υπεύθυνο για την αντιμετώπιση κάθε κινδύνου που αναφέρεται στην έκθεση αξιολόγησης.

Στήλη Δ – Πόροι που απαιτούνται: Στο Σχέδιο Δράσης πρέπει να αναφέρονται οι πόροι που απαιτούνται για την αντιμετώπιση κάθε κινδύνου, οι οποίοι θα πρέπει να υπολογίζονται είτε σε ανθρωποώρες είτε σε χρηματική αξία. Επίσης, προτείνεται ο χαρακτηρισμός της χρηματοδότησης ως 'νέα χρηματοδότηση', 'υπάρχουσα χρηματοδότηση' ή 'επαναδιάθεση χρηματοδότησης'. Αντίστοιχοι δείκτες μπορούν να εφαρμοσθούν για τις ανάγκες σε προσωπικό (π.χ. πρόσληψη νέου προσωπικού, υπάρχον προσωπικό).

Στήλη Ε – Προγραμματισμένη ημερομηνία ολοκλήρωσης: Για κάθε κίνδυνο θα πρέπει να ανατίθεται μία ημερομηνία ολοκλήρωσης των μέτρων αντιμετώπισης. Εάν αυτό συμβεί πριν ή μετά την ημερομηνία αυτή, θα αναφέρεται στη στήλη *Κατάστασης*. Επίσης, εάν ο χρόνος επιδιόρθωσης υπερβεί τον αρχικό προγραμματισμό θα πρέπει να αναφέρονται οι λόγοι της καθυστέρησης στη στήλη *Αλλαγές Σημείων Αναφοράς* μαζί με την αναθεωρημένη ημερομηνία ολοκλήρωσης.

Στήλη ΣΤ – Περιγραφή των Σημείων Αναφοράς: Τα Σημεία Αναφοράς είναι τα συγκεκριμένα αναγκαία μέτρα, *'προσανατολισμένα προς τη δράση',* για την άμβλυνση ενός κινδύνου. Ο αριθμός τους ανά κίνδυνο πρέπει να αντιστοιχεί στον αριθμό των διορθωτικών ενεργειών που απαιτούνται για την πλήρη αντιμετώπιση και επίλυσή του. Πρέπει να έχει τουλάχιστον ένα σημείο αναφοράς για κάθε κίνδυνο και μία ημερομηνία ολοκλήρωσής του, η οποία προσδιορίζει τον προβλεπόμενο χρόνο μέσα στον οποίο θα πρέπει να έχουν γίνει οι διορθωτικές ενέργειες. Με αυτό τον τρόπο τα σημεία αναφοράς μπαίνουν σε μία λογική σειρά.

Τα σημεία αναφοράς πρέπει να αντιστοιχούν στα σημαντικά βήματα για την άμβλυνση ενός κινδύνου. Για παράδειγμα, όταν εντοπίζεται η εξής αδυναμία «ταυτοποίηση και πιο αυστηρές διαδικασίες αυθεντικοποίησης», τα κατάλληλα Σημεία Αναφοράς θα μπορούσαν να είναι τα εξής:

- Αξιολόγηση των μεθόδων για ενίσχυση της ταυτοποίησης και αυθεντικοποίησης,
- Ανάπτυξη διαδικασιών για τυποποίηση της αυθεντικοποίησης,
- Υλοποίηση κατάλληλης αυθεντικοποίησης

Στήλη Ζ – Αλλαγές Σημείων Αναφοράς: στη συγκεκριμένη στήλη καταγράφονται τυχόν διακυμάνσεις στη διαθεσιμότητα των πόρων, στον περιοδικό επαναπροσδιορισμό των δραστηριοτήτων και κάθε απρόβλεπτη καθυστέρηση και έχουν ως αποτέλεσμα την αλλαγή χρονοδιαγράμματος.

Στήλη Η – Κατάσταση (Status): στη συγκεκριμένη στήλη καταγράφονται οι τιμές '*Ολοκληρώθηκε'*, '*Σε εξέλιξη'* ή ' *Καθυστέρηση'*.

Τρίμηνο [Α (ΙΑΝ-ΜΑΡ), Β (ΑΠΡ-ΙΟΥΝ), Γ (ΙΟΥΛ-ΣΕΠ), Δ (ΟΚΤ-ΔΕΚ)]

Σχέδιο Δράσης και Σημείων Αναφοράς-Plan of Action and Milestones (POA&M)							
Αντίμετρο		**Οδηγίες**				**Σχόλια-Παρατηρήσεις**	
Επίπεδο Επιπτώσεων Κινδύνου		Χαμηλό, Μέτριο, Υψηλό					
<Πληροφοριακό Σύστημα>							
Αναγνωριστικό	**Περιγραφή Κινδύνου**	**Σημείο Επαφής-Point of Contact (POC)**	**Απαιτούμενοι πόροι**	**Προγραμματισμένη Ημερομηνία Ολοκλήρωσης**	**Σημεία Αναφοράς (π.χ. δράσεις αποκατάστασης) με ημερομηνίες ολοκλήρωσής τους.**	**Πηγή Εντοπισμού της αδυναμίας**	**Κατάσταση**
Εκχώρηση μοναδικού αναγνωριστικού για κάθε αντικείμενο του POAM	Παροχή λεπτομερούς περιγραφής του κινδύνου	Υπεύθυνο άτομο για την υλοποίηση του έργου	Καθορισμός των απαιτούμενων πόρων (ανθρωποώρες ή χρηματικό κόστος) για την άμβλυνση του κινδύνου. Εάν δεν απαιτούνται νέοι πόροι για την αντιμετώπιση του κινδύνου (μπορεί να επιδιορθωθεί το πρόβλημα με τους υφιστάμενους πόρους) , δήλωση ΚΑΝΕΝΑΣ.	**Το πεδίο είναι μόνιμο και δεν πρέπει να αλλάξει μετάτην έγκριση της διοίκησης.** Επαναπρογραμματισμός στις ημερομηνίες ολοκλήρωσης στη στήλη "Αλλαγές Σημείων Αναφοράς".	**Το πεδίο είναι μόνιμο και δεν μπορεί να αλλάξει μετά την έγκριση της διοίκησης.** Συστάσεις/Επιδιορθώσεις για την αντιμετώπιση του κινδύνου	Η πληροφορία αυτή θα πρέπει να συμβαδίζει με την πληροφορία που συλλέγεται από την αξιολόγηση κινδύνου.	"Σε εξέλιξη", "Καθυστέρηση" ή "Ολοκληρώθηκε" και η ημερομηνία ολοκλήρωσης
1	Δεν έχουν αξιολογηθεί ή ενημερωθεί όλες οι διαδικασίες ελέγχου πρόσβασης που αναφέρονται στο Σχέδιο Ασφαλείας Συστήματος (System Security Plan) τα τελευταία δύο χρόνια. -ΜΕΤΡΙΟΣ ΚΙΝΔΥΝΟΣ	Ανδρέας Σάσσαλος-Υπεύθυνος Ασφαλείας ΠΣ	60 ανθρωποώρες	2/15/2013	Τεκμηριωμένη αξιολόγηση των υφιστάμενων πολιτικών και διαδικασιών ελέγχου πρόσβασης -Access Control SOP(Standard Operation of Access Control). Σχεδιασμός μίας ετήσιας αξιολόγησης των πολιτικών και διαδικασιών ελέγχου πρόσβασης-Ενημέρωση περιεχομένου όπου είναι απαραίτητο .	Αξιολόγηση Ασφαλείας/ Ανάλυση Κινδύνου 01/15/2013, Εύρημα #1	**Ολοκληρώθηκε**: 2/15/2013
2	Το εργαλείο σάρωσης ασφαλείας επιστρέφει->SSL Server Weak Encryption and Communication Vulnerability - ΜΕΤΡΙΟΣ ΚΙΝΔΥΝΟΣ	Ανδρέας Σάσσαλος-Υπεύθυνος Ασφαλείας ΠΣ	30 ανθωποώρες	03/25/2013	Αλλαγή στη λίστα των αλγορίθμων κρυπτογράφησηςπου υποστηρίζονται-προσθήκη του SSLProtocoLDisable SSLv2	Αξιολόγηση Ασφαλείας/ Ανάλυση Κινδύνου 01/15/2013, Εύρημα #2	**Σε εξέλιξη - Προτεραιότητα #1**
3	Η σάρωση της διαδικτυακής εφαρμογής επιστρέφει-OpenSSH Attack Vulnerability (Web Application Scanning (Web Inspect)) - ΥΨΗΛΟΣ ΚΙΝΔΥΝΟΣ	Προμηθευτής	300,00€	10/3/2011	Αναβάθμιση στην τελευταία έκδοση του λειτουργικού συστήματος Διαμόρφωση του συστήματος	Αξιολόγηση Ασφαλείας/ Ανάλυση Κινδύνου 01/15/2013, Εύρημα #3	**Καθυστέρηση:** 03/18/2013

3.3 Μεθοδολογίες Ανάλυσης και Διαχείρισης Κινδύνου

Η Ευρωπαϊκή Υπηρεσία για την Ασφάλεια των δικτύων και της πληροφορίας (European Network and Information Security Agency – ENISA) έχει δημιουργήσει ένα αποθετήριο που περιέχει έναν κατάλογο από μεθόδους διαχείρισης και ανάλυσης κινδύνων. Συνολικά ο κατάλογος αυτός περιέχει δεκατρείς (13) μεθόδους, καθεμία από τις οποίες περιγράφεται σύμφωνα με ένα συγκεκριμένο πρότυπο [6]. Για τις ανάγκες της διατριβής έγινε μία επιλογή τεσσάρων από τις πιο χαρακτηριστικές μεθοδολογίες που περιέχονται στον παραπάνω κατάλογο, για να μελετηθούν και εν συνεχεία παρουσιασθούν. Οι μεθοδολογίες που επιλέχθηκαν και παρουσιάζονται στη συνέχεια είναι η ειδική έκδοση 800-30 του NIST, η CRAMM, η OCTAVE και η EBIOS.

3.3.1 National Institute of Standards and Technology (NIST)

Η ειδική έκδοση 800-30 του αμερικάνικου Εθνικού Ινστιτούτου Προτύπων και Τεχνολογίας, *«Οδηγός Διαχείρισης Επικινδυνότητας στα ΠΣ» (NIST SP 800-30 Risk Management Guide for Information Technology Systems)* περιέχει κατευθυντήριες οδηγίες για τους ομοσπονδιακούς οργανισμούς των ΗΠΑ που επεξεργάζονται ευαίσθητες πληροφορίες και δεδομένα, οι οποίες όμως δεν είναι υποχρεωτικές, ούτε αποτελούν δεσμευτικούς κανόνες, και μπορούν να υιοθετηθούν κάλλιστα και από μη κυβερνητικούς οργανισμούς.

Σύμφωνα με τη συγκεκριμένη μεθοδολογία [19] η διαχείριση κινδύνου αποτελείται από τρεις διαδικασίες: την ανάλυση κινδύνου, την άμβλυνση, και τη συνεχή αξιολόγηση και εκτίμηση. Η αποτελεσματική διαχείριση θα πρέπει να ενσωματώνεται πλήρως στον Κύκλο Ζωής Ανάπτυξης Συστημάτων (System Development Life Cycle-SDLC). Ο κύκλος ζωής ανάπτυξης ενός ΠΣ συνίσταται από τις εξής πέντε φάσεις: έναρξη, ανάπτυξη ή απόκτηση, υλοποίηση, λειτουργία ή συντήρηση, και διάθεση. Η διαχείριση κινδύνου είναι η ίδια ανεξάρτητα από το σε ποια φάση γίνεται η αξιολόγηση. Είναι μία επαναληπτική διαδικασία που μπορεί να πραγματοποιείται κατά τη διάρκεια κάθε σημαντικής φάσης του κύκλου.

Η ανάλυση κινδύνου (risk assessment) είναι η πρώτη διαδικασία της μεθοδολογίας. Οι οργανισμοί χρησιμοποιούν την ανάλυση για τον καθορισμό του εύρους της πιθανής απειλής και κινδύνου σε σχέση με ένα ΠΣ κατά τη διάρκεια του κύκλου ζωής. Το αποτέλεσμα αυτής της διαδικασίας εξυπηρετεί στην λήψη των κατάλληλων μέτρων ελέγχου για τον περιορισμό ή εξαφάνιση του κινδύνου στην επόμενη διαδικασία της άμβλυνσης. Η μεθοδολογία περιλαμβάνει εννέα κύρια βήματα, τα οποία περιγράφονται παρακάτω:

1. **Χαρακτηρισμός Συστήματος:** στο πρώτο βήμα γίνεται ο καθορισμός του πεδίου εφαρμογής, προσδιορίζονται τα όρια του ΠΣ, μαζί με τους πόρους και την πληροφορία που το αποτελούν. Ο χαρακτηρισμός του ΠΣ καθορίζει και το πεδίο εφαρμογής της ανάλυσης κινδύνου και παρέχει την απαραίτητη πληροφορία για τον προσδιορισμό του κινδύνου.
2. **Εντοπισμός Απειλών:** αρχικά εντοπίζονται όλες οι δυνητικές πηγές-απειλών του ΠΣ και αξιολογούνται. Ως πηγή απειλής ορίζεται κάθε κατάσταση ή περιστατικό που ενδεχομένως μπορεί να προκαλέσει ζημιά στο ΠΣ. Ο ανθρώπινος παράγοντας αποτελεί μία επικίνδυνη δυνητικά πηγή-απειλής και σε αυτή την περίπτωση θα πρέπει να εξετάζονται τα κίνητρα και τα μέσα που χρησιμοποιούνται για την διεξαγωγή μίας επίθεσης. Αποτέλεσμα αυτού του βήματος είναι η κατάρτιση ενός δηλωτικού απειλών, στο οποίο αναφέρονται όλες οι πηγές που θα μπορούσαν να εκμεταλλευθούν τις αδυναμίες του ΠΣ.
3. **Εντοπισμός Ευπαθειών:** η ανάλυση των απειλών ενός ΠΣ θα πρέπει να περιλαμβάνει και μία ανάλυση των ευπαθειών που σχετίζονται με το περιβάλλον του. Οι υπαρκτές ευπάθειες συνήθως διαφέρουν ανάλογα με τη φύση του ΠΣ, αλλά και από τη φάση του κύκλου ζωής (SDLC). Ο αποτελεσματικός εντοπισμός των ευπαθειών μπορεί να επιτευχθεί μέσα από προληπτικές μεθόδους, όπως η *χρήση αυτοματοποιημένων εργαλείων σάρωσης*, *έλεγχοι ασφαλείας και αξιολόγηση (security test and evaluation-ST&E)*, και *δοκιμές διείσδυσης (penetration tests)*. Το προσωπικό που διενεργεί την ανάλυση καθορίζει το κατά πόσο οι απαιτήσεις ασφαλείας που προβλέπονται για το ΠΣ και τίθενται κατά τη διάρκεια του χαρακτηρισμού του συστήματος, πληρούνται από τους υφιστάμενους ή προγραμματισμένους ελέγχους ασφαλείας. Αποτέλεσμα

αυτού του βήματος είναι μία λίστα των ευπαθειών (παρατηρήσεων) του ΠΣ που θα μπορούσαν να εκμεταλλευθούν ενδεχομένως οι πηγές-απειλών.

4. **Ανάλυση Ελέγχων:** οι έλεγχοι ασφαλείας εμπεριέχουν τη χρήση τεχνικών και μη μεθόδων. Επίσης, κατατάσσονται σε προληπτικούς (π.χ. έλεγχος πρόσβασης, κρυπτογράφηση, αυθεντικοποίηση) και αστυνομικούς (π.χ. καταγραφές ενεργειών, μέθοδοι ανίχνευσης εισβολών κλπ). Αποτέλεσμα του βήματος είναι η κατάρτιση μίας λίστας με τους τρέχοντες και τους προγραμματισμένους ελέγχους που εφαρμόζονται στο ΠΣ για την άμβλυνση της πιθανότητας εμφάνισης μίας ευπάθειας και μείωση των επιπτώσεων μίας τέτοιας ανεπιθύμητης ενέργειας.
5. **Προσδιορισμός πιθανότητας εμφάνισης:** παράγοντες όπως το κίνητρο και η δυναμικότητα της πηγής-απειλής, η φύση της ευπάθειας, η έκταση και αποτελεσματικότητα των υφιστάμενων ελέγχων θα πρέπει να εξετασθούν στην ταξινόμηση της συνολικής πιθανότητας εμφάνισης. Ο παρακάτω πίνακας περιγράφει τα τρία επίπεδα πιθανότητας εμφάνισης:

Επίπεδο	Ορισμός πιθανότητας εμφάνισης
Υψηλό	Υπάρχει υψηλό κίνητρο και η πηγή-απειλής είναι ικανοποιητικά ικανή, ενώ οι προληπτικοί έλεγχοι είναι αναποτελεσματικοί.
Μέτριο	Υπάρχει κίνητρο και η πηγή-απειλής είναι ικανή, ενώ οι έλεγχοι που εκτελούνται μπορούν να εμποδίσουν την εμφάνιση της ευπάθειας.
Χαμηλό	Δεν υπάρχει κίνητρο και η πηγή-απειλής δεν είναι ικανή, ενώ οι έλεγχοι που εκτελούνται αποτρέπουν ή τουλάχιστον εμποδίζουν σημαντικά την εμφάνιση της ευπάθειας.

6. **Ανάλυση Επιπτώσεων:** σε αυτό το στάδιο απαραίτητες πληροφορίες είναι η αποστολή του ΠΣ (π.χ. ποιες διαδικασίες εκτελεί), η κρισιμότητα του ΠΣ και των δεδομένων (π.χ. η αξία και η σπουδαιότητα του ΠΣ για τον οργανισμό), και τέλος η ευαισθησία του ΠΣ και των δεδομένων. Οι πληροφορίες αυτές μπορούν να ληφθούν από τη υφιστάμενη τεκμηρίωση, όπως οι εκθέσεις ανάλυσης επιπτώσεων στην αποστολή ή οι εκθέσεις αξιολόγησης κρισιμότητας αγαθών. Η πρώτη ανάλυση (επίσης γνωστή και ως ανάλυση επιπτώσεων στην επιχείρηση-business impact analysis) ιεραρχεί τα επίπεδα των επιπτώσεων που συνδέονται με τη διαρροή πληροφοριακών αγαθών του οργανισμού βασιζόμενη πάνω σε μία ποιοτική ή ποσοτική ανάλυση της ευαισθησίας και κρισιμότητας αυτών των αγαθών. Η δεύτερη ανάλυση εντοπίζει και ιεραρχεί τα ευαίσθητα και κρίσιμα πληροφοριακά αγαθά του οργανισμού (π.χ. το υλικό, λογισμικό, συστήματα, υπηρεσίες, λοιπά τεχνολογικά αγαθά) που υποστηρίζουν τις κρίσιμες αποστολές του. Η αρνητική επίπτωση ενός περιστατικού ασφαλείας μπορεί να περιγραφεί υπό τους όρους της απώλειας ή υποβάθμισης ενός ή παραπάνω στόχων ασφαλείας, όπως, η ακεραιότητα, η διαθεσιμότητα και η εμπιστευτικότητα.

Μέγεθος επιπτώσεων	Ορισμός Επίπτωσης
Υψηλό	Η εμφάνιση της ευπάθειας α) μπορεί να οδηγήσει σε ιδιαίτερα δαπανηρές απώλειες σημαντικών αγαθών ή πόρων, β) μπορεί να παραβιάσει, βλάψει ή εμποδίσει σημαντικά την αποστολή του οργανισμού, της φήμης και των συμφερόντων του, γ)μπορεί να οδηγήσει σε απώλεια ανθρώπινης ζωής ή σοβαρό τραυματισμό.
Μέτριο	Η εμφάνιση της ευπάθειας α) μπορεί να οδηγήσει σε δαπανηρές απώλειες αγαθών ή πόρων, β) να παραβιάσει, βλάψει ή εμποδίσει τη αποστολή, φήμη ή τα συμφέροντα του οργανισμού, γ)να προκαλέσει τραυματισμό.
Χαμηλό	Η εμφάνιση της ευπάθειας α)μπορεί να οδηγήσει σε απώλειες αγαθών ή πόρων ,β)να επηρεάσει αισθητά τη αποστολή, φήμη ή τα συμφέροντα του οργανισμού.

7. **Προσδιορισμός Κινδύνου:** στόχος είναι η ανάλυση του επιπέδου του κινδύνου για το ΠΣ. Ο προσδιορισμός του κινδύνου για ένα συγκεκριμένο ζεύγος απειλής/ευπάθειας μπορεί να

εκφρασθεί ως μία συνάρτηση α) της πιθανότητας μίας δεδομένης πηγής-απειλής να εμφανισθεί σε μία δεδομένη ευπάθεια, β) το μέγεθος των επιπτώσεων από την επιτυχή εκμετάλλευση μίας ευπάθειας και γ) την επάρκεια των σχεδιαζόμενων και υφιστάμενων ελέγχων ασφαλείας για τη μείωση ή εξάλειψη του κινδύνου. Για τον υπολογισμό του κινδύνου θα πρέπει να αναπτυχθεί μία κλίμακα κινδύνου και ένας πίνακας επιπέδου κινδύνου.

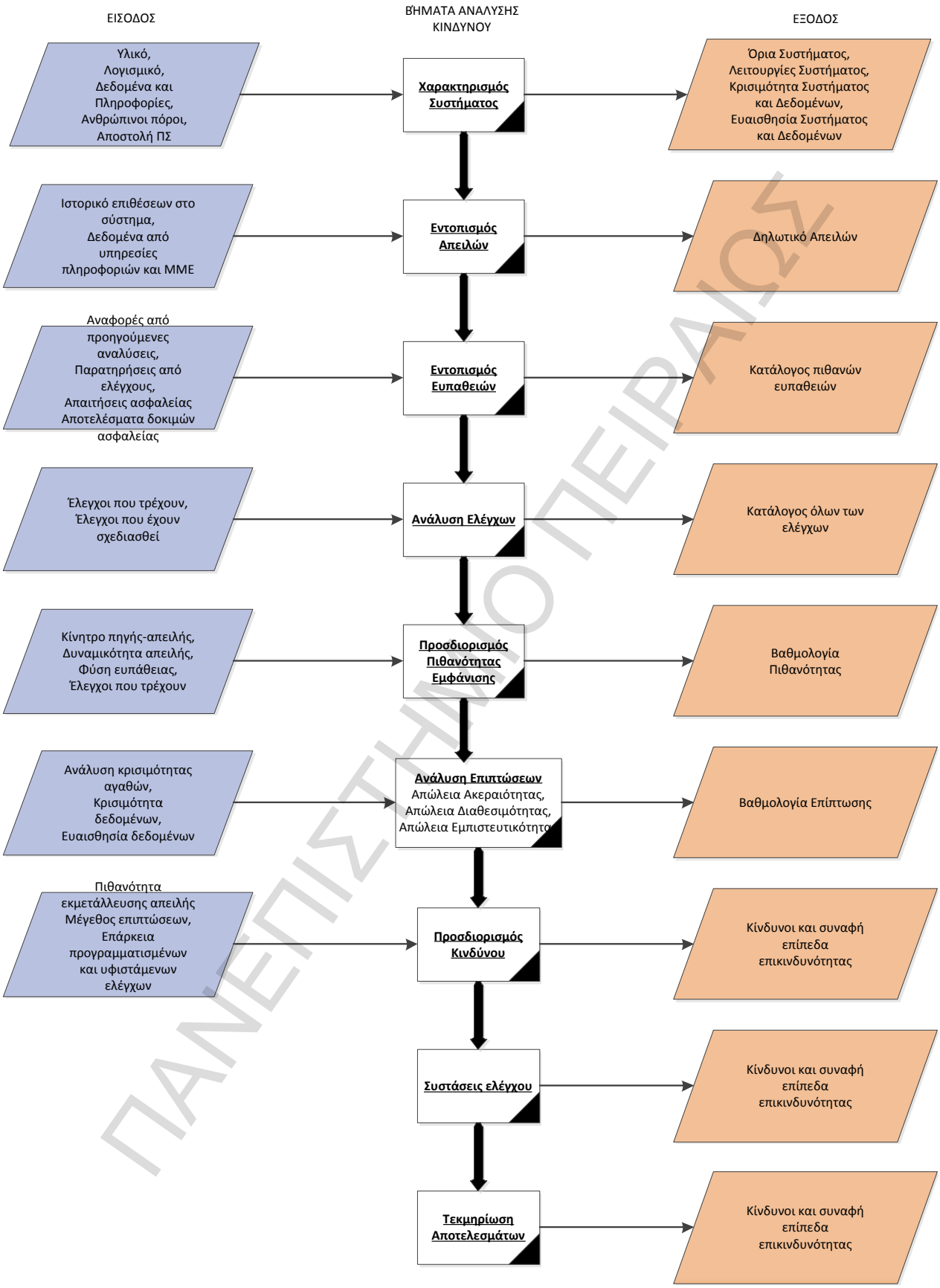
Πιθανότητα εμφάνισης απειλής	**Επίπτωση**		
	Χαμηλή (10)	**Μέτρια** (50)	**Υψηλή** (100)
Υψηλή (1.0)	**Χαμηλός** 10*1.0=10	**Μέτριος** 50*1.0=50	**Υψηλός** 100*1.0=100
Μέτρια (0.5)	**Χαμηλός** 10*0.5=5	**Μέτριος** 50*0.5=25	**Μέτριος** 100*0.5=50
Χαμηλή (0.1)	**Χαμηλός** 10*0.1=1	**Χαμηλός** 50*0.1=5	**Χαμηλός** 100*0.1=10

Πίνακας 6. Πίνακας επιπέδου κινδύνου

Επίπεδο Κινδύνου	**Περιγραφή κινδύνου και αναγκαίες ενέργειες**
Υψηλό	Εάν μία παρατήρηση ή διαπίστωση αξιολογείται ως υψηλού κινδύνου, υπάρχει μεγάλη ανάγκη για λήψη διορθωτικών μέτρων. Το ΠΣ μπορεί να εξακολουθεί να λειτουργεί, αλλά ένα διορθωτικό σχέδιο δράσης πρέπει να τεθεί σε εφαρμογή το συντομότερο δυνατό.
Μέτριο	Εάν μία παρατήρηση αξιολογείται ως μέτριας επικινδυνότητας, απαιτούνται διορθωτικές ενέργειες και ένα σχέδιο θα πρέπει να αναπτυχθεί εντός εύλογου χρονικού διαστήματος.
Χαμηλό	Εάν μία παρατήρηση περιγράφεται ως χαμηλού κινδύνου η καθορισμένη αρχή έγκρισης (Designated Approving Authority-DAA) θα πρέπει να αποφασίσει εάν υπάρχει ανάγκη λήψης διορθωτικών ενεργειών ή εάν ο κίνδυνος είναι αποδεκτός.

Table 7. Κλίμακα Κινδύνου και Αναγκαίες Ενέργειες

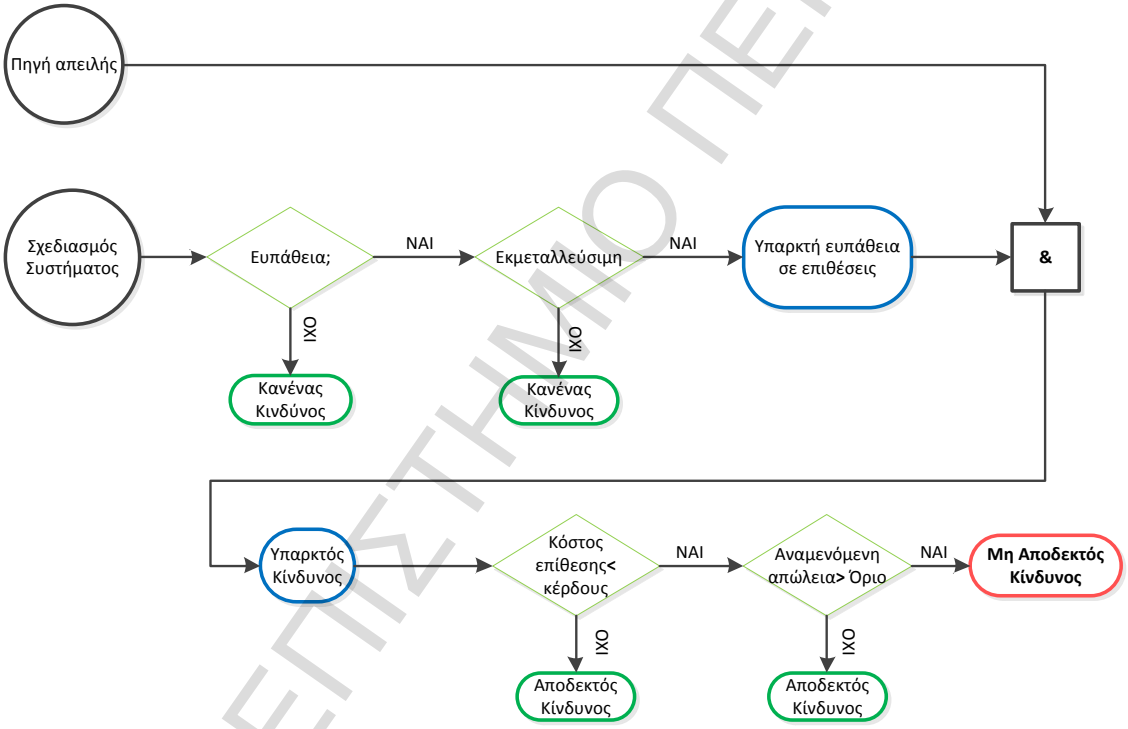
8. **<u>Συστάσεις ελέγχου:</u>** σε αυτό το στάδιο προτείνονται τα μέτρα ελέγχου που πρέπει να ληφθούν για την εξάλειψη ή την ελαχιστοποίηση του κινδύνου. Στόχος είναι η μείωση του κινδύνου που αντιμετωπίζουν τα ΠΣ και τα δεδομένα σε ένα αποδεκτό επίπεδο, λαμβάνοντας υπόψη ορισμένους παράγοντες, όπως, την αποτελεσματικότητα των προτεινόμενων μέτρων (π.χ. συμβατότητα με το ΠΣ), τη νομοθεσία και τους κανονισμούς, την πολιτική του οργανισμού, τις επιπτώσεις στη λειτουργία του και τους κινδύνους ασφαλείας και αξιοπιστίας. Οι συστάσεις είναι τα αποτελέσματα της διαδικασίας ανάλυσης κινδύνου και αποτελούν τα δεδομένα εισόδου της επόμενης διαδικασίας (άμβλυνσης), κατά την οποία γίνεται η αξιολόγηση, ιεράρχηση και εφαρμογή τους.
9. **<u>Τεκμηρίωση Αποτελεσμάτων:</u>** τα αποτελέσματα της ανάλυσης θα πρέπει να τεκμηριώνονται σε μία επίσημη αναφορά., η οποία βοηθά τα ανώτερα στελέχη στη λήψη αποφάσεων όσον αφορά την πολιτική, τα διαδικαστικά, τον προϋπολογισμό και τη λειτουργία των συστημάτων. Σε αντίθεση με μία έκθεση εσωτερικού ελέγχου, δεν έχει στόχο την απόδοση ευθυνών, αλλά μία συστηματική και αναλυτική προσέγγιση των κινδύνων, ώστε η διοίκηση να τους κατανοήσει και να διαθέσει τους πόρους για μείωση και επιδιόρθωση πιθανών απωλειών. Γι' αυτό το λόγο αρκετοί προτιμούν να αναφέρονται στις απειλές/ευπάθειες ως παρατηρήσεις και όχι ως ευρήματα.



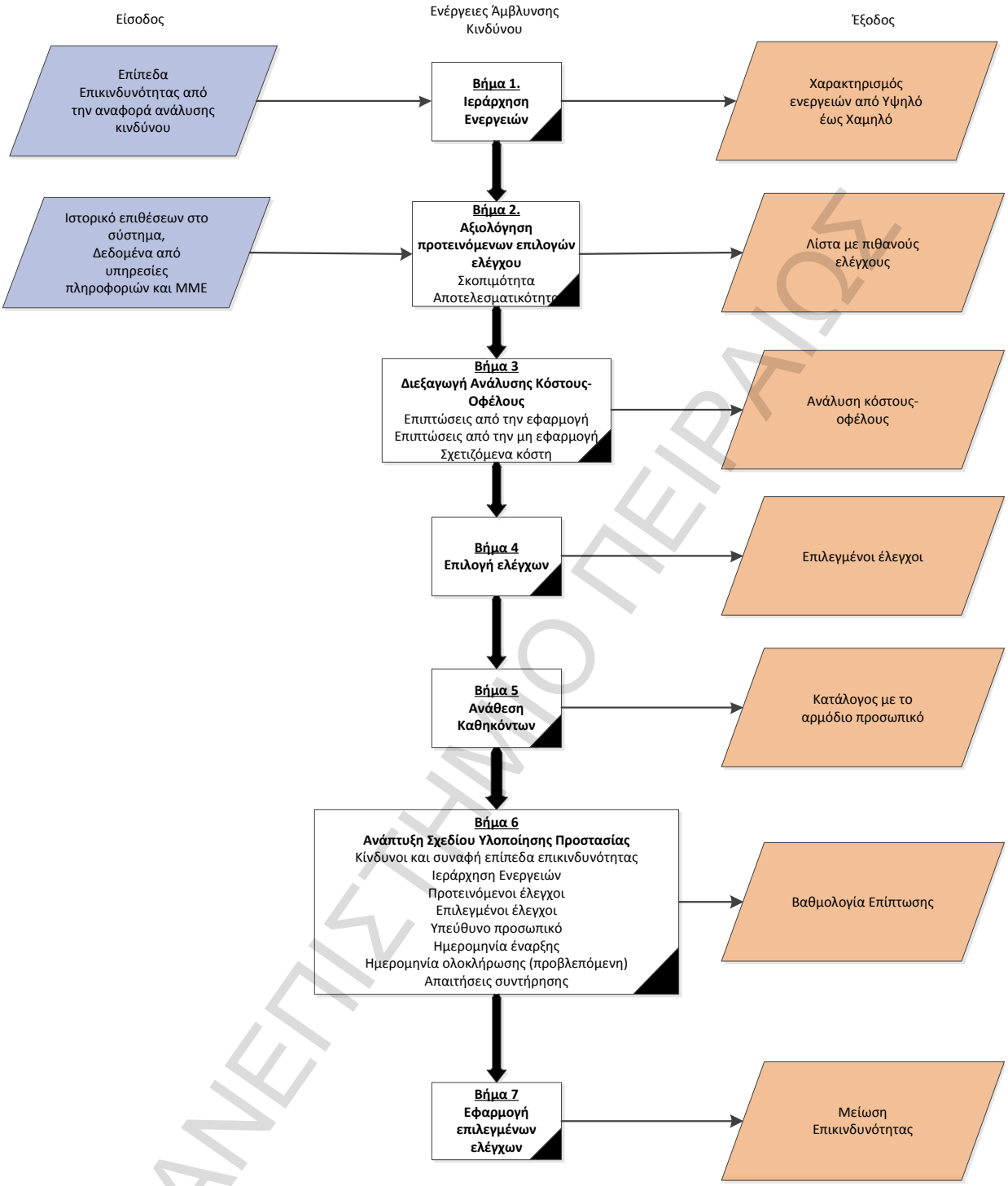
Εικόνα 1. Διάγραμμα Ροής Μεθοδολογίας Ανάλυσης Κινδύνου (NIST SP 800-30).

Η δεύτερη διαδικασία της διαχείρισης κινδύνου, η άμβλυνση (risk mitigation), είναι μία συστηματική μεθοδολογία που χρησιμοποιείται από τη διοίκηση για τον περιορισμό του κινδύνου και η οποία μπορεί να επιτευχθεί μέσα από τις εξής επιλογές:

- **Ανάληψη κινδύνου:** αποδοχή του πιθανού κινδύνου και συνέχιση της λειτουργίας του ΠΣ ή την εφαρμογή μέτρων ελέγχου για μείωσή του σε αποδεκτά επίπεδα.
- **Αποφυγή κινδύνου:** αποφυγή του κινδύνου μέσω της εξάλειψης της αιτίας ή συνέπειας που τον προκαλεί (π.χ. παραίτηση από συγκεκριμένες λειτουργίες του ΠΣ ή τερματισμός μόλις εντοπισθούν οι κίνδυνοι.
- **Περιορισμός κινδύνου:** μέσα από την εφαρμογή μέτρων ελέγχου που ελαχιστοποιούν τις δυσμενείς επιπτώσεις της ανάπτυξης μίας απειλής σε βάρος μίας ευπάθειας (π.χ. χρήση αποτρεπτικών, κατασταλτικών και υποστηρικτικών ελέγχων).
- **Σχέδιο κινδύνου:** ανάπτυξη ενός σχεδίου άμβλυνσης κινδύνου το οποίο ιεραρχεί, εφαρμόζει και τηρεί ελέγχους.
- **Έρευνα και γνώση:** μείωση του κινδύνου απώλειας αναγνωρίζοντας τις ευπάθειες ή τα ελαττώματα και έρευνα για την επιδιόρθωσή τους.
- **Μεταφορά κινδύνου:** χρήση άλλων επιλογών για την αντιστάθμιση της απώλειας, π.χ. ασφαλιστικά συμβόλαια.



Εικόνα 2.Διάγραμμα στρατηγικής άμβλυνσης κινδύνου.



Εικόνα 3. Διάγραμμα Μεθοδολογίας Άμβλυνσης Κινδύνου (NIST SP 800-30).

Κατά την εφαρμογή των προτεινόμενων ελέγχων για τον περιορισμό της επικινδυνότητας, ένας οργανισμός θα πρέπει να εξετάσει την εφαρμογή τεχνικών, λειτουργικών και ελέγχων διαχείρισης ή ακόμα και συνδυασμούς αυτών με στόχο τη μεγιστοποίηση της αποτελεσματικότητας των ελέγχων στα πληροφοριακά του συστήματα. Οι έλεγχοι ασφαλείας με τη σειρά τους, όταν χρησιμοποιούνται ορθά, μπορούν να προλαμβάνουν, να περιορίζουν ή να αποτρέπουν πηγές-απειλών να προκαλέσουν ζημιά στην αποστολή του οργανισμού.

Για την κατανομή των πόρων και την εφαρμογή οικονομικά αποδοτικών ελέγχων, μετά τον εντοπισμό όλων των δυνατών ελέγχων και την αξιολόγηση της σκοπιμότητας και αποτελεσματικότητάς

τους, θα πρέπει να διενεργηθεί μία ανάλυση κόστους-οφέλους για κάθε προτεινόμενο μέτρο ώστε να καθορισθεί ποιοι απαιτούνται και είναι κατάλληλοι για την κάθε περίπτωση. Η ανάλυση κόστους-οφέλους μπορεί να είναι ποιοτική ή ποσοτική. Σκοπός της είναι να αποδείξει ότι το κόστος υλοποίησης των μέτρων δικαιολογείται από τη μείωση του επιπέδου επικινδυνότητας. Για παράδειγμα, ένας οργανισμός δε θα δαπανήσει 1,000€ σε ένα μέτρο για να επιτύχει μείωση του κινδύνου της τάξης των 200€.

Τέλος, επειδή το υφιστάμενο δίκτυο των οργανισμών, θα επεκτείνεται και ανανεώνεται συνεχώς, τα εξαρτήματά του θα αλλάζουν και το λογισμικό/εφαρμογές θα αντικαθίστανται ή ενημερώνονται με νεότερες εκδόσεις, είναι απαραίτητη η συνεχής αξιολόγηση και ανάλυση των νέων συνιστωσών του ΠΣ. Η διαχείριση κινδύνου στα ΠΣ θα πρέπει να διενεργείται και να ενσωματώνεται στον κύκλο ζωής ανάπτυξης συστήματος (SDLC). Επιπλέον, θα πρέπει να υπάρχει προγραμματισμός για την ανάλυση και άμβλυνση των κινδύνων, αλλά αυτή η περιοδική διαδικασία θα πρέπει να είναι εύκαμπτη ώστε να επιδέχεται αλλαγές όταν απαιτείται, όπως σε μεγάλες αλλαγές του ΠΣ ή του περιβάλλοντος επεξεργασίας, εξαιτίας αλλαγών στις πολιτικές ή στις νέες τεχνολογίες.

3.3.2 CRAMM (CCTA Risk Analysis and Management Methodology)

Η Μέθοδος Ανάλυσης και Διαχείρισης Κινδύνου είναι μια ποιοτική ανάλυση επικινδυνότητας, που αναπτύχθηκε από την βρετανική Κεντρική Υπηρεσία Υπολογιστών και Τηλεπικοινωνιών (CRAMM- CCTA Risk Analysis and Management Method) το 1987 και αποτελεί πρότυπο για κυβερνητικούς οργανισμούς του Ηνωμένου Βασιλείου, ενώ πλέον χρησιμοποιείται ευρέως σε περισσότερες από είκοσι (20) χώρες παγκοσμίως, συμπεριλαμβανομένων και ιδιωτικών οργανισμών. Συνοδεύεται από αυτοματοποιημένο εργαλείο λογισμικού που υποστηρίζει όλα τα στάδια της μεθοδολογίας, καθώς και την επιλογή αντιμέτρων [23].

Το ομώνυμο εργαλείο είναι ένα ολοκληρωμένο εργαλείο για τον προσδιορισμό των απαιτήσεων ασφαλείας και έκτακτης ανάγκης, καθώς και την αιτιολόγηση των δαπανών σε συγκεκριμένα αντίμετρα ιδίως όσον αφορά τη λειτουργία ΠΣ.

Στα θετικά του CRAMM συγκαταλέγονται:

- Η δομημένη προσέγγιση της ανάλυσης και διαχείρισης επικινδυνότητας, βασισμένη σε μία καθιερωμένη μέθοδο,
- Η βοήθεια που προσφέρει για το σχεδιασμό ενός σχεδίου έκτακτης ανάγκης, πιστοποίηση ISO 27002, προώθηση ευαισθητοποίησης και αποδοχής σε θέματα ασφάλειας,
- Δυνατότητα πλήρους και ταχείας αξιολόγησης (επιτρέποντας επίσης υψηλού επιπέδου αξιολογήσεις που υποστηρίζουν τις πολιτικές)
- Τακτική ενημέρωση μίας εκτεταμένης ιεραρχικής βάσης αντιμέτρων, που καλύπτουν και μη τεχνικούς τομείς),
- Σχετική σειρά προτεραιότητας των αντιμέτρων, συμπεριλαμβανομένων των κριτηρίων αποτελεσματικότητας και τα κόστη εφαρμογής,
- Συνέπεια που προκύπτει από παρεμφερείς λύσεις για παρόμοια προφίλ κινδύνου.

Στα αρνητικά, από την άλλη συγκαταλέγονται:

- Η ανάγκη για εξειδικευμένους και έμπειρους επαγγελματίες για τη χρήση του εργαλείου,
- Πιθανώς ορισμένα αποτελέσματα σε μία πλήρη αξιολόγηση να είναι ελάσσονος σημασίας, εξαιτίας και της καθυστέρησης μεταξύ της ανάλυσης και της εφαρμογής μετά από ραγδαίες αλλαγές στο σύστημα ή το δίκτυο[24].

Η μέθοδος CRAMM συνίσταται από τρία στάδια, καθένα από τα οποία υποστηρίζεται από στοχευμένα ερωτηματολόγια και οδηγίες [23]. Τα πρώτα δύο στάδια προσδιορίζουν και αναλύουν τους κινδύνους του ΠΣ, ενώ στο τρίτο στάδιο συστήνεται ο τρόπος διαχείρισης των παραπάνω κινδύνων. Τα τρία στάδια της μεθόδου είναι τα εξής:

1. Προσδιορισμός και αποτίμηση αγαθών,
2. Προσδιορισμός απειλών και αδυναμιών, υπολογισμός επικινδυνότητας,
3. Προσδιορισμός και ιεράρχηση αντιμέτρων.

Έναρξη διαδικασίας (ανάλυση επικινδυνότητας)

Η μεθοδολογία εκμεταλλεύεται τις συναντήσεις, τις συνεντεύξεις και τα δομημένα ερωτηματολόγια για τη συλλογή των δεδομένων. Στη φάση έναρξης μίας ανάλυσης, η αρχική συνάντηση των αξιολογητών (το προσωπικό που διενεργεί τις αξιολογήσεις και το οποίο πρέπει να είναι εκπαιδευμένο και έμπειρο στη χρήση του εργαλείου) με τη διοίκηση του οργανισμού είναι σημαντική για τον καθορισμό των στόχων, του πεδίου εφαρμογής και του ορίου της αξιολόγησης, τους όρους αναφοράς, τη δομή του έργου, το χρονοδιάγραμμα και τα παραδοτέα, καθώς και τον εντοπισμό των συνεντευξιαζόμενων. Τα αποτελέσματα αυτής της φάσης τεκμηριώνονται μέσα από ένα «Έγγραφο Έναρξης Έργου».

Προσδιορισμός και Αποτίμηση των Αγαθών (ανάλυση επικινδυνότητας)

Η αξία των αγαθών σε έναν οργανισμό είναι κεντρικής σημασίας για τον προσδιορισμό των κινδύνων και του απαιτούμενου επιπέδου ασφαλείας. Προσδιορίζονται τρείς τύποι αγαθών που συνθέτουν την πληροφορία: τα δεδομένα, το λογισμικό εφαρμογών και τα φυσικά αγαθά (δηλαδή, ο εξοπλισμός, τα κτίρια, το προσωπικό-αξιολογούνται με τις θέσεις που κατέχουν). Με την CRAMM όλα τα συσχετιζόμενα αγαθά, συμπεριλαμβανομένων των υπηρεσιών τελικού χρήστη που διαφοροποιούν την επεξεργασία των δεδομένων (π.χ. διαδραστικές συνεδρίες ηλεκτρονικού ταχυδρομείου, περιήγηση στο Διαδίκτυο), μπορούν να ορισθούν σε μοντέλα αγαθών, και τα οποία αντανακλούν επιχειρησιακές διαδικασίες. Η μοντελοποίηση είναι ένα από τα πιο κρίσιμα ζητήματα στη χρήση του εργαλείου, δεδομένου ότι η υπερβολική ανάλυση σε αυτό το σημείο μπορεί να παρατείνει άσκοπα τη διαδικασία αξιολόγησης, ενώ μέσα από μία επιφανειακή ανάλυση μπορούν να χαθούν σημαντικά αγαθά οδηγώντας έτσι σε παραπλανητικά αποτελέσματα.

Η αποτίμηση των αγαθών θεωρείται ορισμένες φορές ως μία κερδοσκοπική δραστηριότητα, μιας και εξαρτάται από το ποιος (π.χ. ευαίσθητη πληροφορία στα χέρια ενός ανταγωνιστή) και το πότε (π.χ. ληγμένοι κωδικοί) τα κατέχει. Στην CRAMM ο αξιολογητής διενεργεί συνεντεύξεις σε 'ιδιοκτήτες δεδομένων' για να αποτιμήσει τα αγαθά δεδομένων, με αποτέλεσμα την αύξηση της οργανωσιακής αποδοχής της αξιολόγησης. Αυτό το μέρος της αποτίμησης είναι πιο δύσκολο, μιας και είναι δύσκολο να εντοπισθούν οι 'ιδιοκτήτες' των δεδομένων ορισμένες φορές, ή οι συνεντευξιαζόμενοι να χρειάζονται κάποια καθοδήγηση για τους υπολογισμούς τους.

Η αξία προκύπτει από τις επιπτώσεις της παραβίασης της εμπιστευτικότητας, της ακεραιότητας, της διαθεσιμότητας και της μη άρνησης της ευθύνης, δηλαδή των ευρέως διαδεδομένων αρχών της ασφάλειας της πληροφορίας. Οι συνεντευξιαζόμενοι εύλογα περιγράφουν σενάρια της χειρότερης περίπτωσης και υπογραμμίζουν τις πιθανές συνέπειες από τη μη διαθεσιμότητα των δεδομένων (π.χ. για χρονικά διαστήματα από «λιγότερο των δεκαπέντε (15) λεπτών» μέχρι και «άνω των δύο (2) μηνών»), της καταστροφής τους (π.χ. απώλεια των δεδομένων από το τελευταίο αντίγραφο ασφαλείας), της αποκάλυψής τους (εσωτερικά, συμβεβλημένους παρόχους υπηρεσιών, σε ξένους) ή της τροποποίησής τους (π.χ. λάθη πληκτρολόγησης, λανθασμένη έξοδος, εισαγωγή πλαστών μηνυμάτων). Η προσέγγιση αυτή θεωρείται και ως αδυναμία, μιας και τα σενάρια χειρότερης περίπτωσης είναι εξαιρετικά απίθανο να συμβούν στη πραγματικότητα και μπορούν εύκολα να χρησιμοποιηθούν για να διαστρεβλώσουν μία κατάσταση.

Η ορισθείσα βαρύτητα των επιπτώσεων ακολούθως συγκρίνεται με μία κατάλληλη οδηγία (guideline) (π.χ. οικονομική ζημιά/διακοπή δραστηριοτήτων) που παρέχεται από το εργαλείο για την αποτίμηση της αξίας ενός αγαθού σε κλίμακα από το 1 έως το 10. Το προσαρμόσιμο εύρος τιμών (π.χ. '1' για «απώλειες 1,000€ ή λιγότερο», '2' για «απώλειες μεταξύ 1,000€ και 10,000€» κ.ο.κ.) καθορίζονται στις οδηγίες για να αποφευχθεί η δυσκολία λήψης μεμονωμένων υπολογισμών. Για σενάρια οικονομικής απώλειας, η πραγματική ζημία μπορεί επίσης εκτιμηθεί.

Το λογισμικό εφαρμογών καθώς και τα φυσικά αγαθά προφανώς είναι πιο εύκολο να αποτιμηθεί μέσω συνεντεύξεων του προσωπικού υποστήριξης (π.χ. Διευθυντή Πληροφορικής, Διευθυντή εγκαταστάσεων) όσον αφορά το κόστος αντικατάστασης ή ανακατασκευής τους, το οποίο και πάλι μεταφράζεται στην κλίμακα αξιών από 1-10. Εάν το λογισμικό έχει δική του ξεχωριστή απαίτηση για εμπιστευτικότητα ή ακεραιότητα (π.χ. πηγαίος κώδικας λογισμικού κατόπιν παραγγελίας), αποτιμάται όπως τα δεδομένα. Ομοίως συνεπάγεται ότι η αποτίμηση των φυσικών αγαθών και τοποθεσιών, που αποκτώνται για την υποστήριξη δεδομένων και λογισμικού, υπολογίζεται από το εργαλείο.

Προσδιορισμός Απειλών και Αδυναμιών (ανάλυση επικινδυνότητας)

Πρόσθετα με την αποτίμηση αγαθών, τα άλλα δύο βασικά συστατικά της μεθοδολογίας είναι τα επίπεδα (πιθανότητα εμφάνισης) απειλής και αδυναμίας. Οι απειλές και αδυναμίες εξετάζονται απέναντι σε επιλεγμένες ομάδες αγαθών, τα οποία παραμένουν μαζί για ένα εύλογο χρονικό διάστημα επανεξέτασης. Η CRAMM διαθέτει προκαθορισμένους πίνακες για απειλές-ομάδες αγαθών και συνδυασμούς απειλών-επιπτώσεων. Μία εξαντλητική αξιολόγηση κάθε απειλής για κάθε ομάδα αγαθών δεν έχει νόημα και δεν είναι εφικτή, οπότε ο αξιολογητής επιλέγει κατάλληλες απειλές και αγαθά ανάλογα με την περίπτωση. Όσον αφορά τις ευπάθειες-αδυναμίες η CRAMM στοχεύει σε μία διοικητική αξιολόγηση του κινδύνου, παρά σε μία λεπτομερή τεχνική ανάλυση. Συγκεκριμένες αδυναμίες του ΠΣ οι οποίες μπορούν να προσδιορισθούν από σαρωτές ευπαθειών δεν αντιμετωπίζονται από το εργαλείο.

Υπάρχουν δύο τρόποι για την αξιολόγηση των απειλών και των αδυναμιών: η *«πλήρης»* και η *«ταχεία»* εκτίμηση επικινδυνότητας. Στην *«πλήρη»* εκτίμηση, η οποία ως επί των πλείστων συνίσταται, οι απειλές και αδυναμίες προσδιορίζονται μέσα από ερωτήσεις που γίνονται στο προσωπικό υποστήριξης (π.χ. διαχειριστές συστήματος ή δικτύου) με δομημένα ερωτηματολόγια και την εισαγωγή των απαντήσεων στο εργαλείο. Στη συνέχεια, η CRAMM υπολογίζει τα επίπεδα απειλής των αγαθών σε μία κλίμακα πέντε (5) διαβαθμίσεων 'ΠΟΛΥ ΧΑΜΗΛΗ', 'ΧΑΜΗΛΗ', 'ΜΕΤΡΙΑ', 'ΥΨΗΛΗ' ή 'ΠΟΛΥ ΥΨΗΛΗ' καθώς επίσης και τα επίπεδα της ευπάθειας στις απειλές σε κλίμακα 'ΧΑΜΗΛΗ', 'ΜΕΤΡΙΑ' ή 'ΥΨΗΛΗ'. Το στοιχείο της πιθανότητας εμφάνισης υπονοείται στις ερωτήσεις για την εκτίμηση των απειλών και ευπαθειών.

Ένας καλά προετοιμασμένος και έμπειρος αξιολογητής μπορεί επίσης να χρησιμοποιήσει και την *«ταχεία»* εκτίμηση, στην οποία τα επίπεδα απειλής και ευπάθειας εισάγονται απευθείας στο σύστημα με ένα οδηγό αξιολόγησης (π.χ. 'ΠΟΛΥ ΧΑΜΗΛΗ' απειλή για ένα περιστατικό που αναμένεται να εμφανισθεί κατά μέσο όρο όχι περισσότερο από μία φορά κάθε δέκα (10) χρόνια, ή 'ΜΕΤΡΙΑ' ευπάθεια για ένα περιστατικό που αναμένεται να εμφανισθεί με μία πιθανότητα 33% έως 66% στη χειρότερη περίπτωση) παρακάμπτοντας τα αποτελέσματα από τα ερωτηματολόγια. Η ποιοτική προσέγγιση εδώ είναι και η μοναδική επιλογή, μιας και τα πρότυπα, αλλά και οι σχετικές και αξιόπιστες στατιστικές πάνω στις απειλές ή ευπάθειες δεν δύνανται να παράγουν ακριβείς υπολογισμούς.

Υπολογισμός Επικινδυνότητας (ανάλυση επικινδυνότητας)

Η CRAMM υπολογίζει τους κινδύνους για κάθε ομάδα αγαθών έναντι απειλών στις οποίες είναι ευπαθείς σε μία κλίμακα από το ένα (1) έως το επτά (7) χρησιμοποιώντας έναν πίνακα επικινδυνότητας με προκαθορισμένες τιμές, συγκρίνοντας την αξία των αγαθών με τα επίπεδα της απειλής και της ευπάθειας. Σε αυτή την κλίμακα, το '1' υποδηλώνει ένα χαμηλό βασικό επίπεδο απαίτησης ασφαλείας και το '7' ένα πολύ υψηλό επίπεδο.

Το σύστημα μπορεί να αναφέρει ευρήματα τα οποία θα πρέπει να παρουσιαστούν στη διοίκηση για έγκριση προκειμένου να προχωρήσουμε στη φάση της διαχείρισης επικινδυνότητας. Σε αυτό το στάδιο μία συνάντηση επανεξέτασης με τη διοίκηση θα πρέπει να επικεντρωθεί στα πιο σημαντικά ευρήματα(τα οποία θα πρέπει πρώτα να περάσουν από επανεξέταση για τυχόν αποκλίσεις – π.χ. με τη δυνατότητα *"backtrap"*που διαθέτει το εργαλείο- στους υπολογισμούς ή λόγω σφαλμάτων εισόδου), όπως οι υψηλές περιοχές απειλών/ευπαθειών.

CRAMM - Διαχείριση Επικινδυνότητας

Βασιζόμενη στα ευρήματα της ανάλυσης, η CRAMM παράγει ένα σύνολο αντιμέτρων, τα οποία εφαρμόζονται στο σύστημα ή το δίκτυο και τα οποία θεωρούνται απαραίτητα για την αντιμετώπιση των προσδιορισμένων κινδύνων. Το προτεινόμενο προφίλ ασφαλείας θα συγκριθεί με υπάρχοντα αντίμετρα, για τον εντοπισμό περιοχών αδυναμίας ή υπερβολικής πρόνοιας.

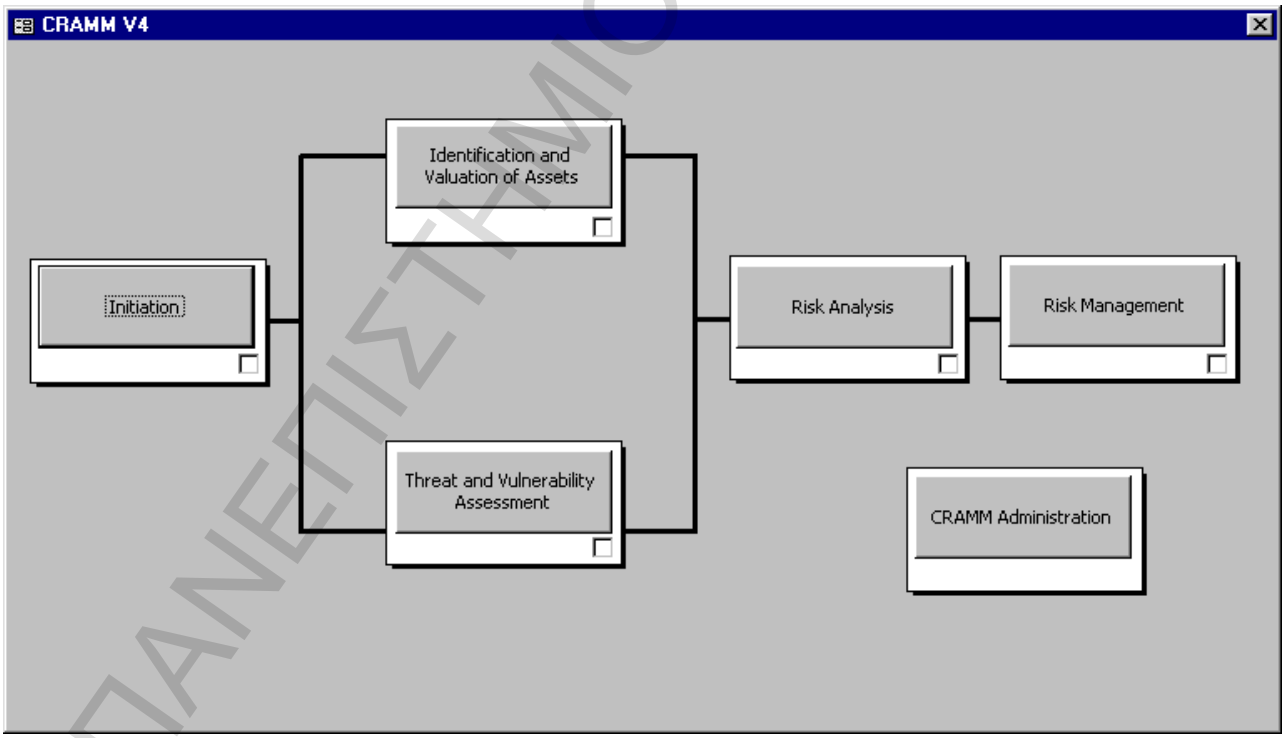
Τα περίπου 4000 αντιμέτρα που προσφέρει η CRAMM συλλέγονται σε ομάδες και υποομάδες, οι οποίες έχουν τις ίδιες παραμέτρους ασφαλείας όπως υλικό, λογισμικό, επικοινωνίες, διαδικασίες, φυσικές εγκαταστάσεις, προσωπικό και περιβάλλον. Επίσης, είναι οργανωμένα σε μία ιεραρχική δομή, σε τρεις διαφορετικές κατηγορίες, από υψηλού επιπέδου στόχους ασφαλείας μέχρι λεπτομερή παραδείγματα εφαρμογής.

Κάθε αντίμετρο φέρει το επίπεδο ασφαλείας σε κλίμακα από '1' (ΠΟΛΥ ΧΑΜΗΛΟ) έως '&' (ΠΟΛΥ ΥΨΗΛΟ) το οποίο επιλέγεται από τη σύγκριση με τη μέτρηση του κινδύνου. Για την υποστήριξη των αποφάσεων της διοίκησης, προτείνεται η χορήγηση προτεραιότητας στα υψηλού επιπέδου αντίμετρα. Ένα από τα πιο δυνατά σημεία της CRAMM είναι ότι βοηθά στη χορήγηση αυτή, δίνοντας σε ένα αντίμετρο υψηλότερη προτεραιότητα όταν:

- Προστατεύει από διάφορες απειλές,
- Απαιτείται για την προστασία ενός συστήματος υψηλού κινδύνου,
- Δεν υπάρχουν εγκατεστημένα εναλλακτικά αντίμετρα,
- Είναι λιγότερο ανέξοδο να εφαρμοσθεί (βάση του γενικού υπολογισμού κόστους),
- Είναι πιο αποτελεσματικό για να πετύχει τους στόχους μίας υποομάδας,
- Αποτρέπει ένα περιστατικό παρά το εντοπίζει ή διευκολύνει στη ανάκτηση.

Η τελευταία δραστηριότητα της CRAMM είναι η παρουσίαση στη διοίκηση μίας περίληψης των ευρημάτων και συμπερασμάτων από την ανάλυση επικινδυνότητας και μίας επεξήγησης των προτεινόμενων αντιμέτρων, παρέχοντας μία γενική ένδειξη στις προτεραιότητες και τα κόστη για την εφαρμογή τους. Η έκθεση αναφοράς της διαχείρισης επικινδυνότητας που παράγει η CRAMM μπορεί επίσης να εξαχθεί για επεξεργασία και μορφοποίηση.

Η δυνατότητα *"what-if"* που προσφέρει η CRAMM επιτρέπει στο χρήστη να αξιολογήσει τις επιπτώσεις των αλλαγών που έχουν πραγματοποιηθεί, καθώς και τις συνέπειες των διαφόρων σεναρίων σχετικά με τις απαιτήσεις ασφαλείας. Εκτός από αρκετές επιλογές του εργαλείου για την εξαγωγή ενημερωτικών εκθέσεων, υπάρχει ενσωματωμένη και η δυνατότητα *"backtrack"* όπως αναφέρθηκε παραπάνω, που παρέχει λόγους (απειλή, ευπάθεια και αξία αγαθού) για την πρόταση κάθε αντιμέτρου ώστε να δικαιολογήσει την επιλογή του.



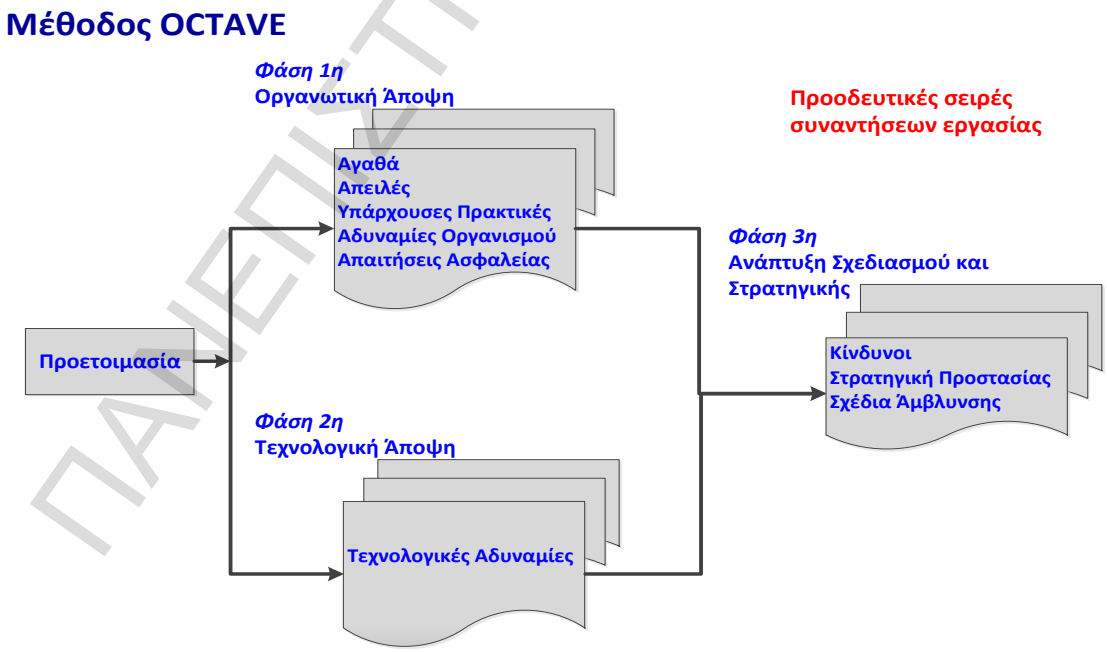
Εικόνα 4. Στιγμιότυπο του εργαλείου CRAMM [23].

3.3.3 OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation)

Η OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) είναι μία **αυτοκατευθυνόμενη (self-directed)** αξιολόγηση ασφάλειας, η οποία αναπτύχθηκε από το Πανεπιστήμιο Carnegie Mellon και η οποία επιτρέπει στους οργανισμούς να κατανοήσουν και αντιμετωπίσουν του κινδύνους ασφαλείας. Η OCTAVE ηγείται από μία μικρή , διεπιστημονική ομάδα, η ομάδα ανάλυσης, η οποία αποτελείται από προσωπικό του ίδιου του οργανισμού και εστιάζει στα αγαθά και τους κινδύνους που αυτά αντιμετωπίζουν. Πρόκειται για μία ολοκληρωμένη, συστηματική, οδηγούμενη από το περιβάλλον (context-driven) προσέγγιση αξιολόγησης. Τα ουσιώδη στοιχεία της προσέγγισης εμπεριέχονται σε ένα σύνολο κριτηρίων που καθορίζουν τις απαιτήσεις της μεθόδου[2].

Η OCTAVE είναι μία προσέγγιση αξιολόγησης βασισμένη σε **συναντήσεις εργασίας** (**workshops**). Μία ανάλυση βασισμένη σε συναντήσεις εργασίας απαιτεί τη συμμετοχή πολλών ανθρώπων για την κατανόηση και εντοπισμό των αγαθών, απειλών και χαρακτηριστικών μίας πληροφοριακής υποδομής. Μία μικρή ομάδα που καλείται ομάδα ανάλυσης (analysis team) καθοδηγεί τη διαδικασία και συγκεντρώνει πληροφορίες μέσα από τη διενέργεια συνεντεύξεων ή συναντήσεων εργασίας. Η ομάδα ανάλυσης εξετάζει και αναλύει αυτές τις πληροφορίες και δημιουργεί σχέδια μείωσης του κινδύνου. Εργαλεία υποστήριξης αποφάσεων μπορούν να χρησιμοποιηθούν για τη διευκόλυνση του έργου της ομάδας, αλλά σε κάθε περίπτωση η ευθύνη για τη λήψη κάθε απόφασης παραμένει στην ομάδα. Η συγκεκριμένη προσέγγιση περιλαμβάνει πολλά μέλη του προσωπικού και μπορεί να είναι χρονοβόρα. Ωστόσο, το προσωπικό του οργανισμού λαμβάνει τις αποφάσεις και κατ' επέκταση κατανοεί και το λόγο λήψης τους.

Η μέθοδος χρησιμοποιεί μία προσέγγιση τριών φάσεων για να εξετάσει τα θέματα του οργανισμού και τα τεχνολογικά θέματα, για τον σχηματισμό μίας ολοκληρωμένης εικόνας των αναγκών ασφαλείας του οργανισμού. Η μέθοδος χρησιμοποιεί συναντήσεις εργασίας που ενθαρρύνουν την ανοικτή συζήτηση και την ανταλλαγή πληροφοριών όσον αφορά τα αγαθά, τις πρακτικές ασφαλείας και τις στρατηγικές. Κάθε φάση αποτελείται από διάφορες διαδικασίες και κάθε διαδικασία έχει μία ή περισσότερες συναντήσεις εργασίας που καθοδηγούνται ή διεξάγονται από την ομάδα εργασίας. Επίσης, είναι απαραίτητες ορισμένες δραστηριότητες προετοιμασίας για να θεμελιώσουν την επιτυχή ολοκλήρωση της αξιολόγησης.



Εικόνα 5. Μέθοδος OCTAVE.

Η **προετοιμασία (preparation)** δημιουργεί τη βάση για μία επιτυχή αξιολόγηση. Ορισμένα σημεία κλειδιά είναι τα εξής:

- Στήριξη από τα ανώτερα κλιμάκια της διοίκησης – πρόκειται για τον πιο κρίσιμο παράγοντα επιτυχίας. Εάν τα ανώτερα διευθυντικά στελέχη υποστηρίζουν τη διαδικασία, τότε το προσωπικό του οργανισμού θα συμμετάσχει ενεργά.
- Επιλογή της ομάδας ανάλυσης – τα μέλη της ομάδας θα πρέπει να διαθέτουν τα κατάλληλα προσόντα για να ηγηθούν της αξιολόγησης. Επιπλέον, θα πρέπει να γνωρίζουν πώς να βγουν από την ομάδα για να διευρύνουν τη γνώση και τις δεξιότητές τους.
- Πεδίο εφαρμογής – η αξιολόγηση θα πρέπει να περιλαμβάνει σημαντικές λειτουργικές μονάδες. Εάν το πεδίο εφαρμογής είναι πολύ μεγάλο, θα είναι δύσκολη η ανάλυση όλων των δεδομένων. Εάν είναι πολύ μικρό, τα αποτελέσματα ενδεχομένως να μην έχουν ιδιαίτερη σημασία.
- Επιλογή συμμετεχόντων – τα μέλη του προσωπικού από πολλαπλά επίπεδα του οργανισμού θα συμβάλουν με τις γνώσεις τους. Σημαντικό είναι τα άτομα αυτά να κατανοήσουν τις λειτουργικές τους περιοχές.

Οι τρείς φάσεις της μεθόδου και οι διαδικασίες τους περιγράφονται παρακάτω.

Φάση 1η : Δημιουργία Προφίλ Απειλών με βάση τα Αγαθά. Πρόκειται για μία οργανωσιακή αξιολόγηση. Η ομάδα ανάλυσης καθορίζει ποια αγαθά είναι περισσότερο σημαντικά στον οργανισμό (κρίσιμα αγαθά) και εντοπίζει τα υπάρχοντα μέτρα προστασίας τους. Οι διαδικασίες της πρώτης φάσης είναι οι εξής:

- Διαδικασία 1 : Προσδιορισμός Γνώσης της Ανώτερης Διοίκησης – Επιλεγμένα ανώτερα στελέχη προσδιορίζουν τα σημαντικά αγαθά, τις αντιληπτές απειλές, τις απαιτήσεις ασφαλείας, τις τρέχουσες πρακτικές ασφαλείας και της οργανωσιακές αδυναμίες.
- Διαδικασία 2 : Προσδιορισμός Γνώσης της Διοίκησης Λειτουργικών Μονάδων - Επιλεγμένοι διευθυντές λειτουργικών μονάδων προσδιορίζουν τα σημαντικά αγαθά, απειλές, απαιτήσεις ασφαλείας, τρέχουσες πρακτικές ασφαλείας και αδυναμίες.
- Διαδικασία 3 : Προσδιορισμός Γνώσης Προσωπικού – Επιλεγμένα μέλη γενικού προσωπικού και προσωπικού πληροφορικής προσδιορίζουν τα σημαντικά αγαθά, απειλές, απαιτήσεις ασφαλείας, τρέχουσες πρακτικές ασφαλείας και αδυναμίες.
- Διαδικασία 4 : Δημιουργία Προφίλ Απειλών – Η ομάδα ανάλυσης επεξεργάζεται την πληροφορία από τις Διαδικασίες 1-3 επιλέγει τα κρίσιμα αγαθά, επαναπροσδιορίζει τις απαιτήσεις ασφαλείας που σχετίζονται με αυτά και προσδιορίζει τις απειλές που αντιμετωπίζουν, δημιουργώντας αντίστοιχα προφίλ.

Φάση 2η : Προσδιορισμός Αδυναμιών Υποδομής. Πρόκειται για μία αξιολόγηση της πληροφοριακής υποδομής. Η ομάδα ανάλυσης εξετάζει τα βασικά λειτουργικά εξαρτήματα για αδυναμίες (τεχνολογικές αδυναμίες) οι οποίες μπορούν να οδηγήσουν σε μη εξουσιοδοτημένη δράση κατά των κρίσιμων αγαθών. Οι διαδικασίες της δεύτερης φάσης είναι οι εξής:

- Διαδικασία 5 : Προσδιορισμός βασικών εξαρτημάτων – Η ομάδα ανάλυσης προσδιορίζει τα βασικά ΠΣ και τα εξαρτήματά τους για κάθε κρίσιμο αγαθό. Στη συνέχεια, επιλέγονται συγκεκριμένες περιπτώσεις για αξιολόγηση.
- Διαδικασία 6 : Αξιολόγηση Επιλεγμένων Εξαρτημάτων – Η ομάδα ανάλυσης εξετάζει τα βασικά συστήματα και εξαρτήματα αυτών για τεχνολογικές αδυναμίες. Εργαλεία εντοπισμού ευπαθειών, όπως λογισμικό, λίστες ελέγχου και scripts χρησιμοποιούνται για αυτό το σκοπό. Τα αποτελέσματα εξετάζονται και συνοψίζονται αναζητώντας τη συνάφεια με τα κρίσιμα αγαθά και τα προφίλ απειλών τους.

Φάση 3η : Ανάπτυξη Στρατηγικής και Σχεδίων Ασφαλείας. Κατά τη διάρκεια αυτού του μέρους της αξιολόγησης, η ομάδα ανάλυσης προσδιορίζει τους κινδύνους που αντιμετωπίζουν τα κρίσιμα αγαθά του οργανισμού και λαμβάνει αποφάσεις. Οι διαδικασίες της τρίτης φάσης είναι οι εξής:

- Διαδικασία 7 : Διεξαγωγή Ανάλυσης Επικινδυνότητας – Η ομάδα ανάλυσης προσδιορίζει τις επιπτώσεις των απειλών στα κρίσιμα αγαθά, δημιουργεί συγκεκριμένα κριτήρια για την

αξιολόγηση των κινδύνων και αξιολογεί τις επιπτώσεις με βάση αυτά τα κριτήρια. Η διαδικασία αυτή παράγει ένα προφίλ κινδύνου για κάθε κρίσιμο αγαθό.

- Διαδικασία 8 : Ανάπτυξη Στρατηγικής Προστασίας – Η ομάδα ανάλυσης δημιουργεί μία στρατηγική προστασίας του οργανισμού και σχέδια άμβλυνσης της επικινδυνότητας, με βάση μίας ανάλυσης της πληροφορίας που συλλέχτηκε. Τα ανώτερα στελέχη στη συνέχεια αναθεωρούν, επεξεργάζονται και εγκρίνουν τη στρατηγική και τα σχέδια.

Μετά την OCTAVE. Τέλος, με την ολοκλήρωση της αξιολόγησης, θα πρέπει να προστεθούν λεπτομέρειες εφαρμογής στη στρατηγική προστασίας και στα σχέδια άμβλυνσης επικινδυνότητας. Οι διευθυντές θα πρέπει επίσης να ορίσουν τα βήματα για τη συνεχή αναθεώρηση και βελτίωση της στρατηγικής ασφαλείας.

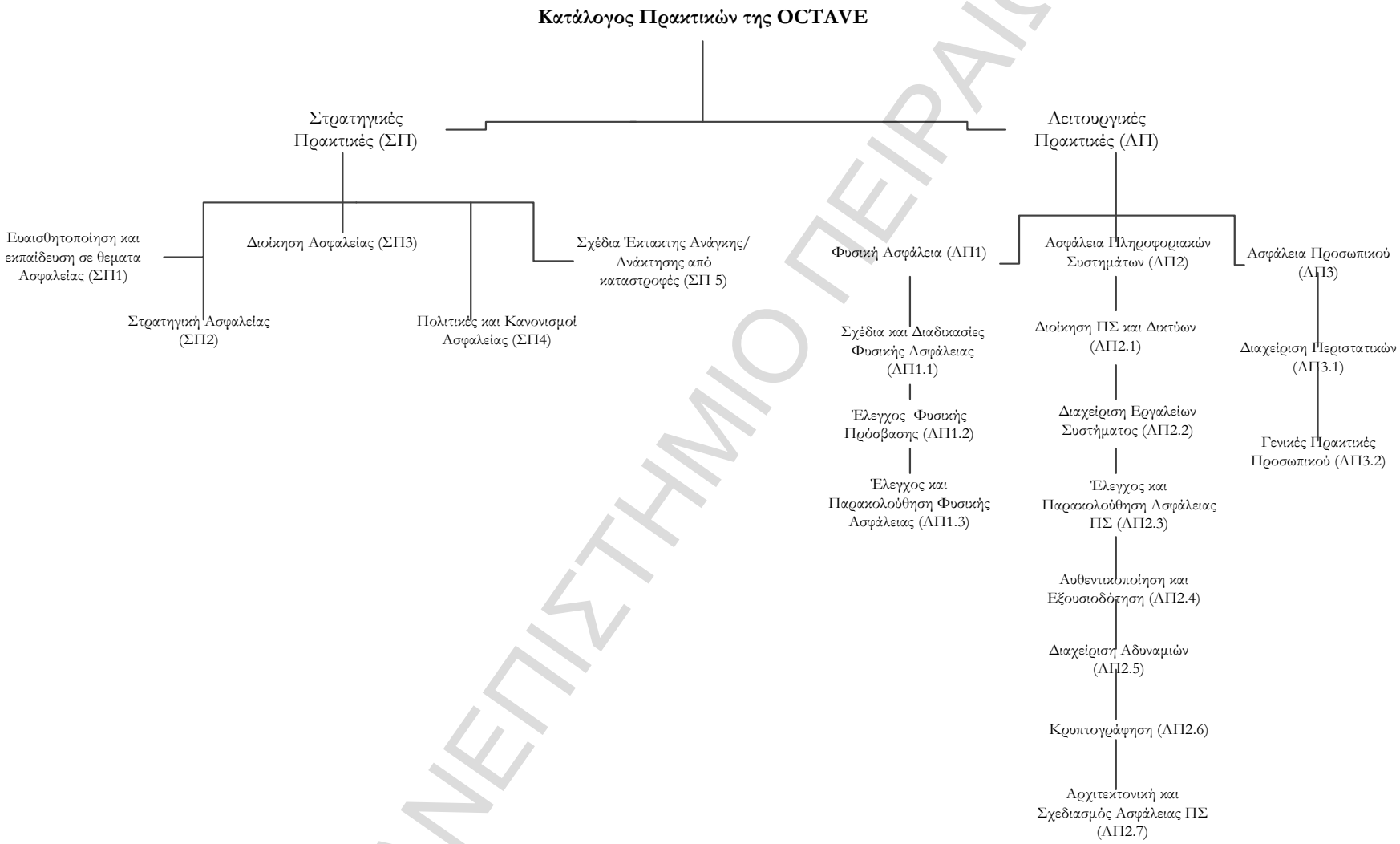
Η OCTAVE χρησιμοποιεί έναν κατάλογο καλών πρακτικών ασφαλείας, ο οποίος παρέχει τα μέσα για τη αξιολόγηση των υφιστάμενων πρακτικών σε έναν οργανισμό και τη δημιουργία μίας στρατηγικής βελτίωσής τους με στόχο την προστασία των κρίσιμων αγαθών. Ο κατάλογος διαιρείται σε δύο τύπους πρακτικών – τις στρατηγικές και τις λειτουργικές. Οι στρατηγικές εστιάζουν σε θέματα οργάνωσης, στις πολιτικές ασφαλείας και προσφέρουν καλές, γενικές πρακτικές διοίκησης. Οι λειτουργικές εστιάζουν σε τεχνολογικά ζητήματα, και πως οι άνθρωποι χρησιμοποιούν, αλληλεπιδρούν και προστατεύουν την τεχνολογία.

Ο κατάλογος πρακτικών (Εικ.6) χρησιμοποιείται πρωταρχικά σε δύο φάσεις της μεθόδου. Στην $1^{η}$ φάση χρησιμοποιείται στις διαδικασίες 1-3., οι οποίες χαρακτηρίζονται ως συνεδρίες εκμαίευσης γνώσης, όπου οι συμμετέχοντες συνεισφέρουν τη γνώση τους σε ζητήματα σχετικά με την ασφάλεια. Μία από τις δραστηριότητες στις διαδικασίες 1-3 είναι ο προσδιορισμός των υφιστάμενων πρακτικών και των αδυναμιών στην οργάνωση μέσα από οπτική γωνία των συμμετεχόντων στις συνεδρίες. Ο κατάλογος επίσης, χρησιμοποιείται στη διαδικασία 8 της μεθόδου, όπου αναπτύσσονται η στρατηγική προστασίας και τα σχέδια άμβλυνσης της επικινδυνότητας. Πρόσθετα, οι πρακτικές του καταλόγου χρησιμοποιούνται ως αναφορά κατά την επιλογή των ενεργειών για τα σχέδια άμβλυνσης από την ομάδα ανάλυσης.

OCTAVE-S

Η ανάπτυξη της OCTAVE-S είχε ως στόχο να εισάγει μία προσέγγιση της OCTAVE σε μικρότερους οργανισμούς, με προσωπικό της τάξεως των 100 ατόμων και κάτω. Πρόκειται για μία προσέγγιση που είναι σύμφωνη με τα κριτήρια της OCTAVE και αποτελείται από τρείς παρόμοιες φάσεις. Ωστόσο, εκτελείται από μία ομάδα ανάλυσης, η οποία έχει εκτεταμένη γνώση του οργανισμού. Έτσι, η OCTAVE-S δε βασίζεται σε επίσημες συνεδρίες εκμαίευσης γνώσης για τη συλλογή της πληροφορίας, μιας και υποτίθεται ότι η ομάδα ανάλυσης (η οποία συνήθως αποτελείται από τρία μέχρι πέντε άτομα) έχει πρακτική γνώση της σημαντικής πληροφορίας που σχετίζεται με τα αγαθά, τις απαιτήσεις ασφαλείας, τις απειλές και τις πρακτικές του οργανισμού [21].

Μία άλλη σημαντική διαφοροποίηση της OCTAVE-S είναι ότι πρόκειται για μία πιο δομημένη μέθοδο. Οι έννοιες ασφαλείας ενσωματώνονται στα φύλλα εργασίας και τους οδηγούς της μεθόδου, επιτρέποντας με αυτόν τον τρόπο στους λιγότερο έμπειρους σε θέματα κινδύνων και ασφάλειας συμμετέχοντες να αντιμετωπίζουν ένα ευρύτερο φάσμα κινδύνων με τους οποίους δεν έχουν οικειότητα. Το χαρακτηριστικό που διακρίνει τη μέθοδο είναι ότι απαιτεί λιγότερο εκτεταμένη εξέταση της πληροφοριακής υποδομής του οργανισμού. Λόγω του ότι οι μικροί οργανισμοί πιθανώς να μη διαθέτουν τους πόρους και τα κατάλληλα εργαλεία εντοπισμού ευπαθειών, η OCTAVE-S σχεδιάστηκε για να περιλαμβάνει μία περιορισμένη εξέταση των κινδύνων της υποδομής, ώστε να εξαλειφθεί το δυνητικό εμπόδιο της αποδοχής τους.



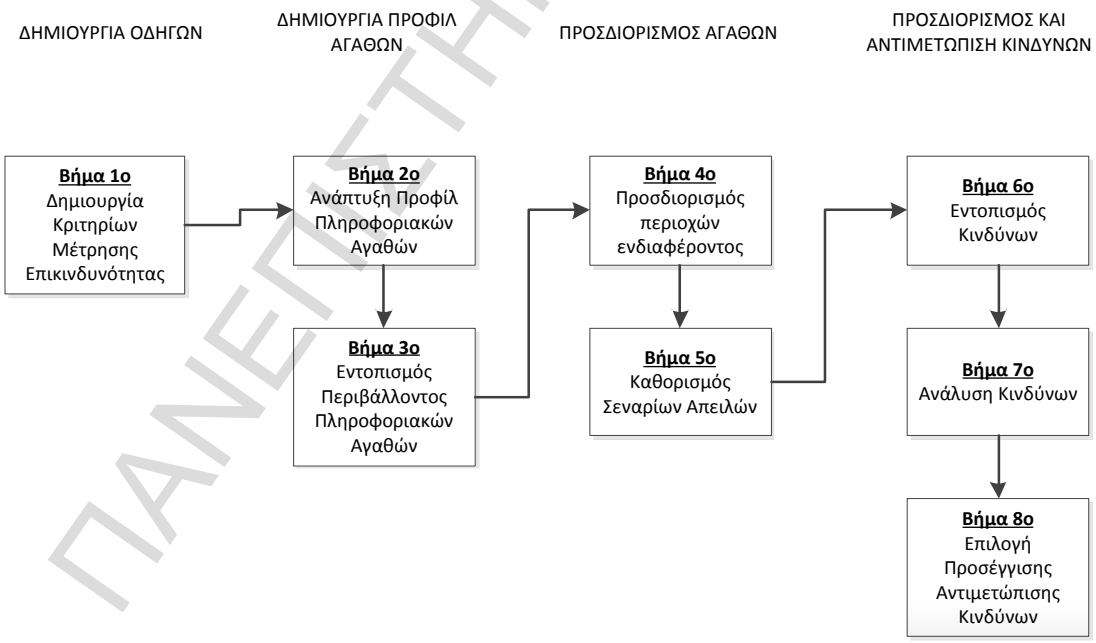
Εικόνα 6. Δομή του Καταλόγου Πρακτικών.

OCTAVE Allegro

Η OCTAVE Allegro εκδόθηκε το 2007 και πρόκειται για την επόμενη γενιά της μεθόδου, η οποία δεν προορίζεται όμως να αντικαταστήσει τις προηγούμενες μεθοδολογίες. Πρόκειται για μία παραλλαγή η οποία παρέχει μία εξορθολογισμένη διαδικασία που επικεντρώνεται στα πληροφοριακά αγαθά. Ωστόσο κάθε μεθοδολογία έχει ευρεία εφαρμοσιμότητα και οι χρήστες μπορούν να επιλέξουν την προσέγγιση που ταιριάζει καλύτερα στις ανάγκες τους. Η συγκεκριμένη μεθοδολογία είναι σχεδιασμένη για να επιτρέπει ευρύτερη αξιολόγηση του περιβάλλοντος επικινδυνότητας του οργανισμού με στόχο την παραγωγή καλύτερων αποτελεσμάτων, χωρίς την ανάγκη για εκτεταμένη γνώση ανάλυσης επικινδυνότητας [21].

Η διαφοροποίησή της από τις προηγούμενες προσεγγίσεις έγκειται στο ότι εστιάζει στα πληροφοριακά αγαθά και κυρίως στο περιβάλλον που αυτά χρησιμοποιούνται, αποθηκεύονται, μεταφέρονται και επεξεργάζονται, καθώς και στο τρόπο που εκτίθενται σε απειλές, στις αδυναμίες τους με αποτέλεσμα τη διακοπή της λειτουργίας τους. Όπως και οι προηγούμενες προσεγγίσεις μπορεί να εκτελεστεί μέσω συνεδρίων, σε ένα συνεργατικό περιβάλλον και υποστηρίζεται από φύλλα εργασίας και ερωτηματολόγια. Ωστόσο, η OCTAVE Allegro είναι επίσης κατάλληλη για χρήση από μεμονωμένα άτομα που θέλουν να κάνουν ανάλυση επικινδυνότητας χωρίς εκτεταμένη συμμετοχή του οργανισμού και ιδιαίτερη εμπειρία.

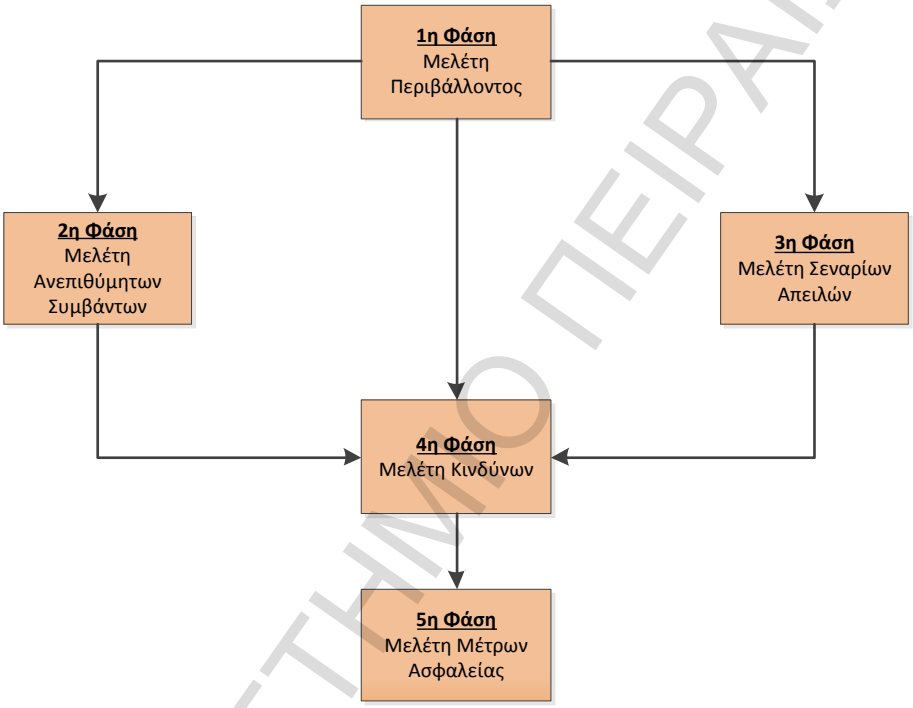
Η OCTAVE Allegro αποτελείται από οκτώ (08) βήματα τα οποία οργανώνονται σε τέσσερις (04) φάσεις, όπως φαίνεται στο παρακάτω σχήμα. Στην 1η φάση, ο οργανισμός αναπτύσσει τα κριτήρια μέτρησης επικινδυνότητας σύμφωνα με την οργανωτική του δομή. Κατά τη διάρκεια της 2ης φάσης, δημιουργείται το **προφίλ (asset profiling)** για τα πληροφοριακά αγαθά που καθορίζονται ως κρίσιμα. Η διαδικασία χαρακτηρισμού τους καθορίζει σαφή όρια για το κάθε αγαθό, προσδιορίζει τις απαιτήσεις ασφαλείας και εντοπίζει όλες τις τοποθεσίες αποθήκευσης, μεταφοράς και επεξεργασίας του. Στην 3η φάση, προσδιορίζονται οι απειλές του αγαθού μέσα στο προηγούμενο περιβάλλον τοποθεσιών. Στην 4η και τελευταία φάση προσδιορίζονται και αναλύονται οι κίνδυνοι που αντιμετωπίζουν το αγαθό και ξεκινά η ανάπτυξη του σχεδιασμού άμβλυνσής τους.



Εικόνα 7. Τα Βήματα της Μεθοδολογίας OCTAVE Allegro

3.3.4 EBIOS – Expression des Besoins et Identification des Objectifs de Sécurité

Η Εθνική Υπηρεσία για την Ασφάλεια των Πληροφοριακών Συστημάτων (L'Agence nationale de la sécurité des systèmes d'information-ANSSI) του Υπουργείου Αμύνης της Γαλλίας ανέπτυξε και διατηρεί μία σημαντική μεθοδολογία για να βοηθήσει τους οργανισμούς του δημοσίου τομέα, αλλά και του ιδιωτικού στη διαχείριση ασφάλειας των ΠΣ τους. Η μεθοδολογία αποτελείται από βέλτιστες πρακτικές και λογισμικό. Η μεθοδολογία EBIOS είναι ένα ολοκληρωμένο εργαλείο για τη διαχείριση της επικινδυνότητας και είναι σύμφωνη με το διεθνές πρότυπο ISO/IEC 27001:2005 [7]. Η μεθοδολογία εισάγει μία διαδικασία διαχείρισης της επικινδυνότητας που αποτελείται από πέντε φάσεις, όπως φαίνονται και στο παρακάτω σχήμα:



Εικόνα 8. Μεθοδολογία EBIOS.

Η διαδικασία είναι επαναληπτική, δηλαδή, θα πρέπει να γίνει αρκετές φορές μέχρι να ολοκληρωθεί η κάθε φάση, ώστε να υπάρχει σταδιακή βελτίωση του περιεχομένου και η συνολική προσέγγιση να τελειοποιηθεί [7] [18].

1η Φάση-Μελέτη του Περιβάλλοντος: στην πρώτη φάση δημιουργείται το πλαίσιο διαχείρισης του κινδύνου, δηλαδή, καθορίζονται ο τρόπος μέτρησης της επικινδυνότητας και το εύρος της μελέτης, τα κρίσιμα πληροφοριακά αγαθά, οι φορείς στους οποίους ανήκουν και προσδιορίζονται οι παράμετροι που πρέπει να ληφθούν υπόψη για την αντιμετώπιση των κινδύνων. Με την ολοκλήρωση της πρώτης φάσης το εύρος της μελέτης περιορίζεται, ενώ περιγράφονται με σαφήνεια όλοι οι παράμετροι που πρέπει να εξεταστούν στις επόμενες φάσεις. Η πρώτη φάση αποτελείται από τις παρακάτω δραστηριότητες οι οποίες με τη σειρά τους περιλαμβάνουν συγκεκριμένες δράσεις:

- **Δραστηριότητα 1.1 –** Ορισμός του πλαισίου της διαχείρισης κινδύνων.
  - Δράση 1.1.1 – Χάραξη της μελέτης των κινδύνων.
  - Δράση 1.1.2 – Περιγραφή του γενικού πλαισίου.
  - Δράση 1.1.3 – Οριοθέτηση του πεδίου μελέτης.
  - Δράση 1.1.4 – Προσδιορισμός των παραμέτρων που πρέπει να ληφθούν υπόψη.
  - Δράση 1.1.5 – Προσδιορισμός των πηγών απειλής.
- **Δραστηριότητα 1.2 –** Προετοιμασία των Μετρικών.

- Δράση 1.2.1 – Καθορισμός απαιτήσεων ασφαλείας και ανάπτυξη κλίμακας αναγκών.
- Δράση 1.2.2 – Ανάπτυξη κλίμακας βαρύτητας.
- Δράση 1.2.3 – Ανάπτυξη κλίμακας περιγραφής όλων των δυνατών επιπέδων πιθανότητας εμφάνισης των σεναρίων απειλής.
- Δράση 1.2.4 – Ορισμός κριτηρίων για τη διαχείριση κινδύνων.

- **Δραστηριότητα 1.3** – Προσδιορισμός των Αγαθών.
  - Δράση 1.3.1 – Προσδιορισμός των κρίσιμων αγαθών.
  - Δράση 1.3.2 – Προσδιορισμός των συστατικών των ΠΣ (τεχνικά και μη) που υποστηρίζουν τα κρίσιμα αγαθά της προηγούμενης Δράσης και τους 'ιδιοκτήτες αυτών'.
  - Δράση 1.3.3 – Καθορισμός της σχέσης μεταξύ των κρίσιμων αγαθών και των αγαθών υποστήριξης.
  - Δράση 1.3.4 – Εντοπισμός των υφιστάμενων και προγραμματισμένων μέτρων ασφαλείας.

2η Φάση-Μελέτη Ανεπιθύμητων συμβάντων: η δεύτερη φάση συμβάλει στην αξιολόγηση των κινδύνων. Εντοπίζει και αξιολογεί τις ανάγκες ασφαλείας των βασικών αγαθών (όσον αφορά τη διαθεσιμότητα, ακεραιότητα και εμπιστευτικότητα) και τις επιπτώσεις (στην αποστολή του οργανισμού, την προσωπική ασφάλεια, οικονομικά και νομικά ζητήματα,…) σε περίπτωση μη συμμόρφωσης με τις απαιτήσεις αυτές από περιστατικά που μπορούν να προκληθούν από πηγές-απειλών (όπως ανθρώπινες, περιβαλλοντικές, εσωτερικές, εξωτερικές, εκούσιες, ακούσιες,…).

- **Δραστηριότητα 2.1** – Αξιολόγηση των επίφοβων περιστατικών.
  - Δράση 2.1.1 – Ανάλυση όλων των επίφοβων περιστατικών.
  - Δράση 2.1.2 – Αξιολόγηση κάθε επίφοβου περιστατικού.

3η Φάση-Μελέτη Σεναρίων Απειλών: η τρίτη φάση αποτελεί επίσης μέρος της αξιολόγησης των κινδύνων. Προσδιορίζει και αξιολογεί σενάρια που μπορούν να προκαλέσουν περιστατικά ασφαλείας. Για να γίνει αυτό εξετάζονται οι πηγές-απειλών που μπορούν να δημιουργήσουν ή εκμεταλλευτούν **ευπάθειες** των συστημάτων του οργανισμού.

- **Δραστηριότητα 3.1** – Αξιολόγηση των σεναρίων απειλών.
  - Δράση 3.1.1 – Ανάλυση όλων των σεναρίων απειλών.
  - Δράση 3.1.2 – Αξιολόγηση κάθε σεναρίου απειλής

4η Φάση-Μελέτη Κινδύνων: η τέταρτη φάση αναδεικνύει τους κινδύνους που αντιμετωπίζει ο οργανισμός και για τους οποίους υπάρχει ο φόβος. Επίσης, περιγράφεται ο τρόπος που γίνεται η εκτίμηση και αξιολόγηση των κινδύνων, και τέλος, προσδιορίζονται οι **στόχοι ασφαλείας** που πρέπει να επιτευχθούν.

- **Δραστηριότητα 4.1 –** Αξιολόγηση των κινδύνων.
  - Δράση 4.1.1 – Ανάλυση κινδύνων (αναγνώριση όλων των κινδύνων και καθορισμός της βαρύτητας και πιθανότητάς τους, αρχικά ανεξάρτητα από τα υφιστάμενα μέτρα ασφάλειας και σε δεύτερο χρόνο λαμβάνοντάς τα υπόψη).
  - Δράση 4.1.2 – Εκτίμηση κινδύνων (σε αυτή τη δράση γίνεται μία εκτίμηση της σημασίας των κινδύνων και ανάλογα με τα κριτήρια διαχείρισης επικινδυνότητας που χρησιμοποιούνται γίνεται η ιεράρχησή τους).
- **Δραστηριότητα 4.2 –** Προσδιορισμός στόχων ασφαλείας.
  - Δράση 4.2.1 – Επιλογή τρόπου αντιμετώπισης κινδύνων (καθορίζεται και το επίπεδο του υπολειπόμενου κινδύνου το οποίο είναι αποδεκτό).
  - Δράση 4.2.2 – Ανάλυση του εναπομείναντος κινδύνου (προσδιορίζονται και γίνεται εκτίμηση των κινδύνων που εξακολουθούν να υφίστανται αφότου έχουν επιτευχθεί όλοι οι στόχοι ασφαλείας και υπάρχει πλήρης γνώση της αποδοχής τους).

5η Φάση-Μελέτη Μέτρων Ασφάλειας: στην πέμπτη και τελευταία φάση προσδιορίζονται τα μέτρα για την αντιμετώπιση των κινδύνων, αλλά και ο εναπομένων κίνδυνος μετά την εφαρμογή τους.

- **Δραστηριότητα 5.1** – Επισημοποίηση των μέτρων ασφαλείας που πρέπει να εφαρμοσθούν.
    - Δράση 5.1.1 – Καθορισμός μέτρων ασφαλείας.
    - Δράση 5.1.2 – Ανάλυση του εναπομείναντος κινδύνου.
    - Δράση 5.1.3 – Δήλωση εφαρμογής των μέτρων.
- **Δραστηριότητα 5.2** – Εφαρμογή μέτρων ασφαλείας.
    - Δράση 5.2.1 – Ανάπτυξη σχεδίου δράσης και παρακολούθηση της εφαρμογής των μέτρων ασφαλείας.
    - Δράση 5.2.2 – Ανάλυση του εναπομείναντος κινδύνου.
    - Δράση 5.2.3 – Χορήγηση έγκρισης ασφαλείας (ουσιαστικά πρόκειται για την επικύρωση των αποτελεσμάτων της μελέτης – είναι η δέσμευση της αρχής πιστοποίησης ότι η μελέτη έχει λάβει υπόψη όλους τους λειτουργικούς περιορισμούς και ότι το ΠΣ και η πληροφορία προστατεύονται σύμφωνα με τους στόχους ασφαλείας).

4. Μελέτη Περίπτωσης – Βιβλιοθήκη και Κέντρο Πληροφόρησης

4.1 Εισαγωγή

Για την πραγματοποίηση της παρούσας μελέτης επιλέχθηκε και χρησιμοποιήθηκε η μέθοδος EBIOS - Expression des Besoins et Identification des Objectifs de Sécurité (Έκφραση Αναγκών και Καθορισμός Στόχων Ασφαλείας), η οποία αναπτύχθηκε από την Εθνική Υπηρεσία για την Ασφάλεια των Πληροφοριακών Συστημάτων του Γαλλικού Υπουργείου Αμύνης, καθώς και το ομώνυμο βοηθητικό εργαλείο. Το εργαλείο βοηθά το χρήστη να εκτελέσει όλα τα βήματα της ανάλυσης και διαχείρισης κινδύνου σύμφωνα με τις πέντε (5) φάσεις της μεθόδου και επιτρέπει την καταγραφή των αποτελεσμάτων της μελέτης καθώς και την παραγωγή όλων των απαιτούμενων έγγραφων αναφορών (reports). Το εργαλείο EBIOS , το οποίο βρίσκεται στη $2^{η}$ έκδοση, επιλέχθηκε διότι είναι ανοιχτού κώδικα και προσφέρεται δωρεάν, και παράλληλα εναρμονίζεται πλήρως με τις βέλτιστες πρακτικές που προτείνονται από το Διεθνές πρότυπο ISO/IEC 27001/27002.

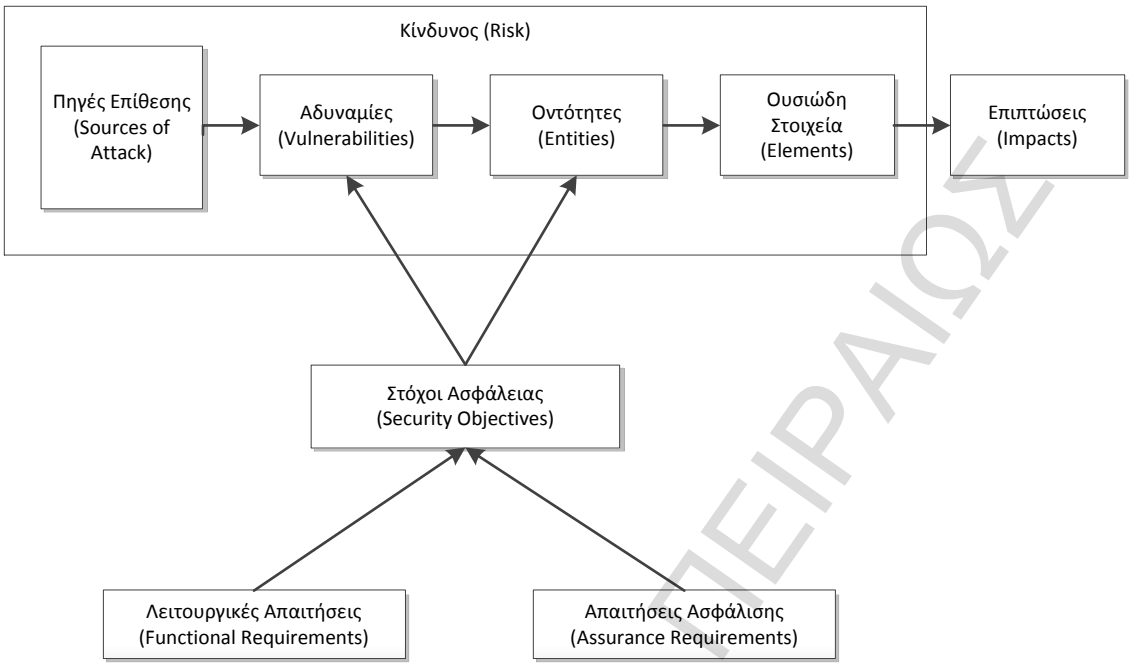
Σύμφωνα με τη μεθοδολογία EBIOS [11] ένα πληροφοριακό σύστημα βασίζεται στα **ουσιώδη στοιχεία (essential elements)** του, δηλαδή στις λειτουργίες (**functions**) του και στην πληροφορία (**information**), τα οποία συνιστούν την προστιθέμενη αξία που έχει το ΠΣ για τον οργανισμό. Τα ουσιώδη στοιχεία συνδέονται με μία σειρά από διάφορους τύπους **οντοτήτων (entities)** όπως: το υλικό, το λογισμικό, τα δίκτυα, άλλους οργανισμούς, το προσωπικό και τις τοποθεσίες.

Προκειμένου να διασφαλιστεί η σωστή επιχειρησιακή λειτουργία του οργανισμού, θα πρέπει να εκφράζεται η ευαισθησία (sensitivity) του κάθε ουσιώδους στοιχείου. Η έκφραση αυτή βασίζεται σε διάφορα **κριτήρια ασφαλείας (security criteria)** όπως η διαθεσιμότητα, η ακεραιότητα και η εμπιστευτικότητα. Εάν η ευαισθησία αυτή δεν καλύπτεται, θα υπάρχουν **επιπτώσεις (impacts)** στον οργανισμό, όπως, οικονομικές απώλειες, μειωμένη δραστηριότητα, απώλεια της εμπιστοσύνης των πελατών, μειωμένη ασφάλεια για το προσωπικό, ρύπανση κλπ, ανάλογα πάντα με τη φύση του ίδιου του οργανισμού.

Κάθε οργανισμός εκτίθεται σε διάφορους **παράγοντες απειλών (threat agents)** οι οποίοι προέρχονται από το περιβάλλον στο οποίο δραστηριοποιείται, την κουλτούρα του, την εικόνα του, το πεδίο δράσης του κλπ. Ένας παράγοντας απειλής μπορεί να χαρακτηριστεί από τον **τύπο (type)** του (φυσικός, ανθρώπινος, περιβαλλοντικός) και από την **αιτία (cause)** που τον προκαλεί (τυχαίο ή εσκεμμένο γεγονός). Είναι δυνατόν να χρησιμοποιηθούν διάφοροι **μέθοδοι επίθεσης (attack methods)** και γι' αυτό το λόγο θα πρέπει να εντοπισθούν. Μία μέθοδος επίθεσης χαρακτηρίζεται από τα κριτήρια ασφαλείας (διαθεσιμότητα, ακεραιότητα, εμπιστευτικότητα κλπ) που παραβιάζει και από τους παράγοντες απειλής που ενδέχεται να τις χρησιμοποιήσουν. Κάθε οντότητα έχει **αδυναμίες (vulnerabilities)** που μπορούν να αξιοποιηθούν από τους παράγοντες απειλών χρησιμοποιώντας κάποια μέθοδο επίθεσης.

Το μόνο που απομένει είναι να καθορισθεί πως τα ουσιώδη στοιχεία μπορούν να επηρεαστούν από τους παράγοντες απειλής και τις μεθόδους επίθεσής τους, δηλαδή ο **κίνδυνος (risk)**. Ο κίνδυνος αντιπροσωπεύει την πιθανή ζημιά και προκύπτει από το γεγονός ότι ένας παράγοντας απειλής μπορεί να επηρεάσει τα ουσιώδη στοιχεία του ΠΣ χρησιμοποιώντας κάποια μέθοδο επίθεσης για να εκμεταλλευτεί μία αδυναμία των οντοτήτων στις οποίες βασίζεται. Οι **στόχοι ασφάλειας (security objectives)** περιλαμβάνουν κυρίως την κάλυψη των αδυναμιών που αφορά τον εναπομείναντα κίνδυνο. Προφανώς, δεν υπάρχει νόημα να προστατευθεί ό, τι δεν εκτίθεται. Ωστόσο, όσο η πιθανότητα επίθεσης αυξάνεται, ανάλογα θα πρέπει να αυξάνεται η αυστηρότητα των στόχων ασφαλείας. Οι στόχοι αυτοί, επομένως, αποτελούν ένα απόλυτα προσαρμοσμένο σύνολο προδιαγραφών.

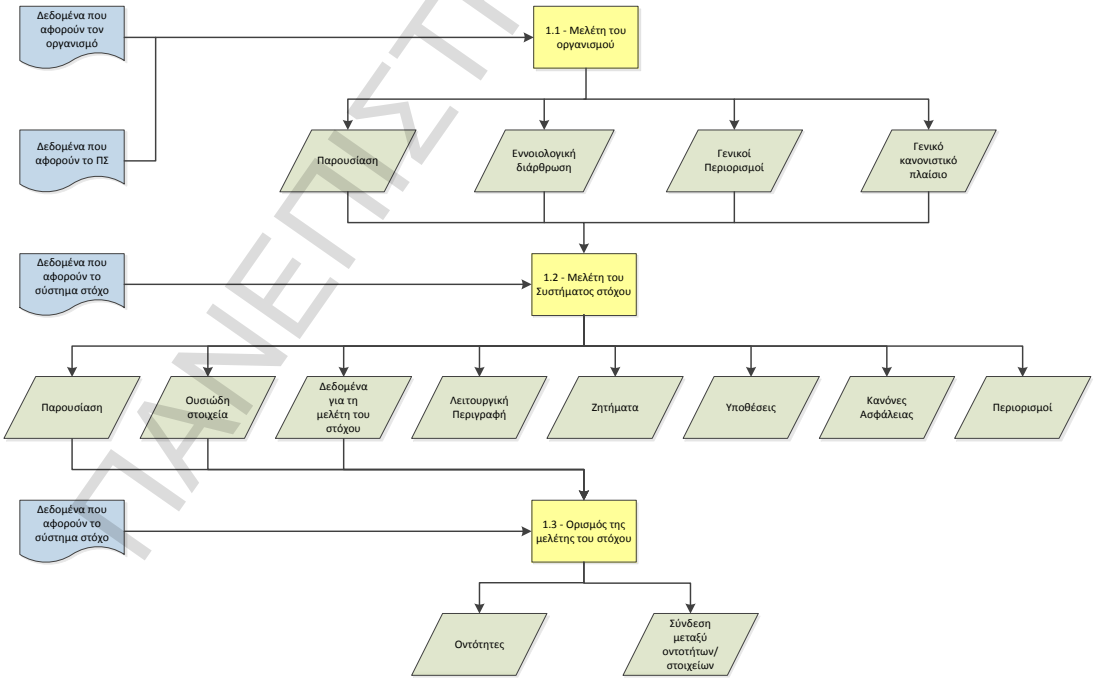
Η ομάδα που είναι υπεύθυνη για την εφαρμογή της προσέγγισης, θα πρέπει να παράγει ακριβείς προδιαγραφές των απαιτούμενων λειτουργιών ασφάλειας. Στη συνέχεια, θα πρέπει να παρουσιάσει ότι οι στόχοι ασφαλείας καλύπτονται τέλεια από τις συγκεκριμένες **λειτουργικές απαιτήσεις (functional requirements)**. Τέλος, η υπεύθυνη ομάδα θα πρέπει να προσδιορίσει τις **απαιτήσεις ασφάλισης (assurance requirements)** που επιτρέπουν την τήρηση του απαιτούμενου επιπέδου εμπιστοσύνης.



Εικόνα 9. Γενικό διάγραμμα ροής μεθοδολογίας EBIOS.

4.1 Βήμα 1 – Μελέτη Γενικού Πλαισίου

Το 1^{ο} βήμα διαιρείται σε τρείς επιμέρους δραστηριότητες (**activities**) οι οποίες αναλυτικά φαίνονται στο παρακάτω διάγραμμα ροής: 1) στη μελέτη του οργανισμού, 2) τη μελέτη του στοχευμένου συστήματος και 3) τον ορισμό του στόχου της μελέτης ασφάλειας[9].



Εικόνα 10. Διάγραμμα ροής Μελέτης Γενικού Πλαισίου.

4.1.1 Μελέτη του οργανισμού (Δραστηριότητα 1.1)

Παρουσίαση του Οργανισμού

Η μελέτη περίπτωσης αφορά τη Βιβλιοθήκη και Κέντρο Πληροφόρησης του Πρότυπου Πανεπιστημίου. Πρόκειται για μία αυτοτελή, ενιαία και αποκεντρωμένη Υπηρεσία η οποία από διοικητική άποψη αντιστοιχεί με Διεύθυνση. Η ΒΚΠ αποτελεί κέντρο συλλογής και διάχυσης της πληροφορίας και έχει σαν σκοπό την υποστήριξη και προώθηση του εκπαιδευτικού και ερευνητικού έργου που επιτελείται στο Πρότυπου Πανεπιστήμιο μέσω της διάθεσης τεκμηριωμένης πληροφορίας, σε κάθε είδους μορφή (βιβλία, μη έντυπο υλικό, ηλεκτρονικό υλικό, νόμιμη πρόσβαση σε υπηρεσίες δικτύου) καθώς, την εκπαίδευση των χρηστών και την ανάπτυξη των δεξιοτήτων τους στη χρήση νέων τεχνολογιών και τη σωστή επιλογή των πηγών πληροφόρησης. Η πληροφορία αυτή είναι στη διάθεση του κοινού της ευρύτερης περιοχής και στη διάθεση άλλων βιβλιοθηκών.

Στόχοι της ΒΚΠ μεταξύ άλλων είναι: α) η επιλογή, η απόκτηση, η οργάνωση και η διαχείριση συλλογών βιβλίων, περιοδικών (έντυπων και ηλεκτρονικών), βάσεων δεδομένων και οπτικοακουστικού υλικού, β) η προάσπιση του δικαιώματος πρόσβασης στην πληροφορία και την προστασία των προσωπικών δεδομένων των χρηστών της, γ) η μέριμνα για την εξασφάλιση του εξοπλισμού (λογισμικού και υλικοτεχνικού) για την ομαλή και απρόσκοπτη λειτουργία της, δ) η υιοθέτηση και εφαρμογή εθνικών και διεθνών προτύπων οργάνωσης και λειτουργίας Βιβλιοθηκών, ε) η υποστήριξη και η πληροφόρηση όλων των χρηστών, στ) η ανάπτυξη του ρόλου της βιβλιοθήκης ως φορέα της εκπαίδευσης από απόσταση και της δια βίου εκπαίδευσης.

Οργάνωση και Δομή Οργανισμού

Η ΒΚΠ στεγάζεται σε δικό της κτήριο στο χώρο του Πρότυπου Πανεπιστημίου και έχει λειτουργική οργανωτική δομή (functional structure):

1. *Διεύθυνση*: η Διοίκηση του συνόλου της ΒΚΠ ασκείται από τον Διευθυντή της Βιβλιοθήκης ο οποίος έχει την ευθύνη της α) της διοίκησης όλου του προσωπικού, β) της διαχείρισης όλων των οικονομικών πόρων που διατίθενται στη Βιβλιοθήκη , σύμφωνα με τους κανόνες και τις αποφάσεις της Διοίκησης του Πανεπιστημίου, γ) της εκπόνησης του ετήσιου απολογισμού της ΒΚΠ, δ) της συνεχής ενημέρωσης και εκπαίδευσης τόσο του προσωπικού όσο και των χρηστών της ΒΚΠ, ε) της επίβλεψης και αποτελεσματικής εκτέλεσης των εργασιών διαχείρισης και καθημερινής λειτουργίας της ΒΚΠ, στ) της εισήγησης του προϋπολογισμού της.
2. *Τμήμα Διοίκησης και Γραμματείας*: είναι υπεύθυνο για τη γραμματειακή υποστήριξη της Διεύθυνσης. Μεριμνά για τη διακίνηση της εισερχόμενης και εξερχόμενης αλληλογραφίας και την τήρηση πρωτοκόλλου εισερχόμενων και εξερχόμενων εγγράφων. Είναι υπεύθυνο για τη διευθέτηση όλων των θεμάτων που αφορούν το προσωπικό της ΒΚΠ, καθώς και για την εγγραφή/ διαγραφή χρηστών. Παράλληλα, μεριμνά για την προβολή του έργου της Βιβλιοθήκης κα έχει την ευθύνη της διοργάνωσης συνεδρίων, ημερίδων, εκδηλώσεων, εκπαιδευτικών σεμιναρίων και της επιμέλειας κάθε έντυπου υλικού της Βιβλιοθήκης.
3. *Τμήμα Οικονομικής Διαχείρισης*: διεκπεραιώνει σε συνεργασία με την Οικονομική Υπηρεσία και την Επιτροπή Ερευνών του Πανεπιστημίου, όλες τις διαδικασίες που απαιτούνται για διαγωνισμούς και τις πληρωμές όλων των τιμολογίων. Διαχειρίζεται τα έσοδα της Βιβλιοθήκης από τις δραστηριότητές της, από δωρεές ή άλλους πόρους. Επίσης, συγκεντρώνει, ελέγχει, συντονίζει και εκτελεί όλες τις παραγγελίες υλικού της ΒΚΠ. Παραλαμβάνει και καταγράφει όλο το υλικό της Βιβλιοθήκης και το προωθεί στο τμήμα Προσκτήσεων και Τεκμηρίωσης.
4. *Τμήμα Προσκτήσεων και Τεκμηρίωσης*: εκτελεί την επεξεργασία του υλικού της Βιβλιοθήκης, εισάγει τα στοιχεία στο σύστημα αυτοματοποίησης της Βιβλιοθήκης HORIZON και εκτυπώνει τα barcodes. Εφαρμόζει τους κανόνες δημιουργίας καθιερωμένων όρων (authorities). Εκτελεί τον έλεγχο των εισαγόμενων και εξαγόμενων εγγραφών προς και από το Συλλογικό Κατάλογο Ακαδημαϊκών Βιβλιοθηκών, χαράζει πολιτική για τις περιπτώσεις που δεν καλύπτονται από τα γενικά πρότυπα (πολιτική καταλογογράφησης). Επίσης, συγκεντρώνει προτάσεις για την αγορά περιοδικών και επιβλέπει τη βιβλιοθηκονομική επεξεργασία τους. Μεριμνά για τη σύνδεση της Βιβλιοθήκης με εθνικά και διεθνή κέντρα πληροφόρησης. Ερευνά για νέες ηλεκτρονικές πηγές πληροφόρησης. Επιμελείται σε συνεργασία με το τμήμα Πληροφοριακών Συστημάτων την ανάπτυξη εφαρμογών ψηφιακής βιβλιοθήκης.

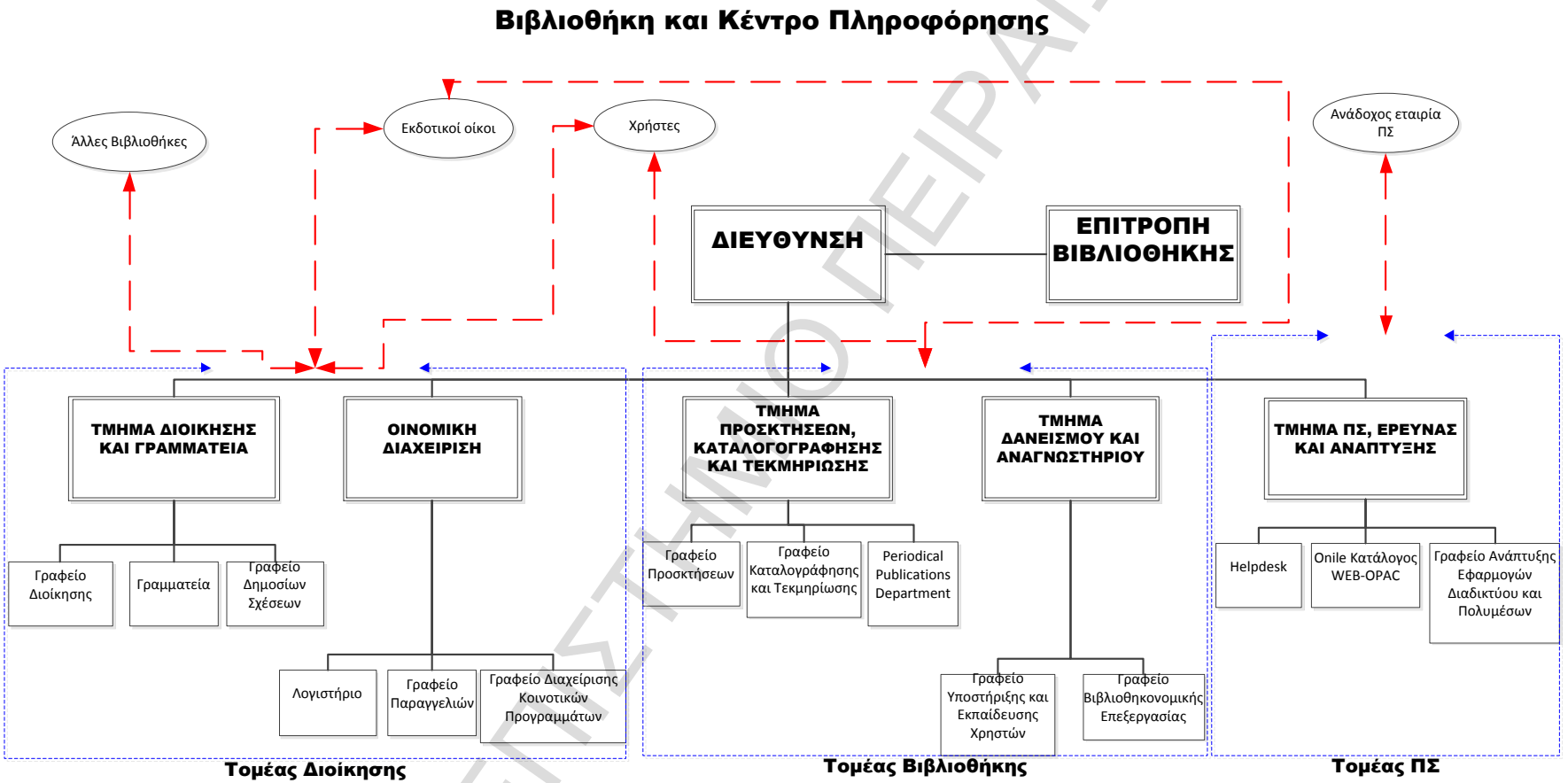
5. <u>Τμήμα Δανεισμού και Αναγνωστηρίου</u>: το τμήμα προσφέρει υπηρεσίες δανεισμού, εξυπηρέτησης χρηστών, διαδανεισμού, βιβλιογραφικής αναζήτησης. Μεριμνά για την καλή λειτουργία των Αναγνωστηρίων και είναι υπεύθυνο για τη φύλαξη και το διαρκή έλεγχο των βιβλίων. Είναι υπεύθυνο για την παρακολούθηση των επιστροφών του δανεισμένου υλικού και την αποστολή υπομνηστικών για το καθυστερημένο υλικό.
6. <u>Τμήμα Πληροφοριακών Συστημάτων</u>: έχει την ευθύνη για τις παραλαβές και εγκαταστάσεις υλικού και λογισμικού, τις αναβαθμίσεις παλαιών Η/Υ, την παραμετροποίηση των επιμέρους λογισμικών και γενικότερα για την καλή λειτουργία των Η/Υ της ΒΚΠ. Επίσης, μεριμνά για τη συντήρηση και παραμετροποίηση του συστήματος αυτοματοποίησης της βιβλιοθήκης (library information system-lis) HORIZON σε συνεργασία πάντα με την ανάδοχο εταιρία. Έχει την ευθύνη για την ανάπτυξη και εξέλιξη εφαρμογών διαδικτύου. Εκτελεί την υποστήριξη του ηλεκτρονικού Helpdesk και λιστών ηλεκτρονικού ταχυδρομείου. Αναπτύσσει online βοηθήματα εκπαίδευσης. Τέλος, έχει την ευθύνη για την ανάπτυξη εφαρμογών ψηφιακής βιβλιοθήκης.

<u>Περιορισμοί που επηρεάζουν τον οργανισμό</u>

1. <u>*Περιορισμοί στον προϋπολογισμό:*</u> αν και δεν είναι κατάλληλη η προσέγγιση στην ασφάλεια με βάση το κόστος, πρέπει να αναφερθεί πως ήδη η ΒΚΠ έχει κάνει μεγάλη προσπάθεια όσον αφορά τον τομέα των πληροφοριακών συστημάτων και κάθε πρόσθετη επένδυση θα πρέπει να είναι πλήρως αιτιολογημένη στις οικονομικές υπηρεσίες.
2. <u>*Περιορισμοί που προκύπτουν από το ημερολόγιο του οργανισμού*</u>: Η περίοδος αιχμής της ΒΚΠ είναι από τον Σεπτέμβριο έως τον Ιούνιου έκαστου έτους, γι' αυτό το λόγο κάθε ενέργεια (εγκατάσταση ενός συστήματος ασφάλειας, εκπαίδευση κλπ) θα πρέπει να γίνει εκτός της περιόδου αυτής.
3. <u>*Περιορισμοί που αφορούν το προσωπικό:*</u> α) το προσωπικό πλην όσων εργάζονται στο τμήμα ΠΣ έχουν περιορισμένες γνώσεις στους η/υ, β) το προσωπικό καθαρισμού εργάζεται από τις 7 έως τις 8 π.μ.
4. <u>*Περιορισμοί από τη φύση του οργανισμού:*</u> α) αρκετά από τα μέλη του προσωπικού έχουν ορισμένου χρόνου σχέσης εργασίας, β) αρκετοί φοιτητές απασχολούνται στη βιβλιοθήκη κάνοντας την πρακτική τους άσκηση είτε από το ίδιο το Πανεπιστήμιο είτε από άλλα.
5. <u>*Οικονομικοί Περιορισμοί*</u>: η ΒΚΠ πέραν από τα όποια έσοδα έχει από τις δραστηριότητές της ή κάποιες δωρεές, ανήκει στο Πανεπιστήμιο και για οποιαδήποτε νέα επένδυση θα πρέπει να λάβει την έγκριση της Επιτροπής Βιβλιοθήκης και των Πρυτανικών Αρχών.

<u>Κανονισμοί που εφαρμόζονται</u>

Η ΒΚΠ λειτουργεί μέσα στο πλαίσιο που ορίζεται από τον Κανονισμό Λειτουργίας της στον οποίο ορίζονται οι κανόνες συμπεριφοράς μέσα στη βιβλιοθήκη, τα δικαιώματα των χρηστών και οι προσφερόμενες υπηρεσίες. Πέραν του κανονισμού αυτού εφαρμογή έχει και η κείμενη νομοθεσία που αφορά την προστασία των δεδομένων προσωπικού χαρακτήρα και την προστασία των πνευματικών δικαιωμάτων.

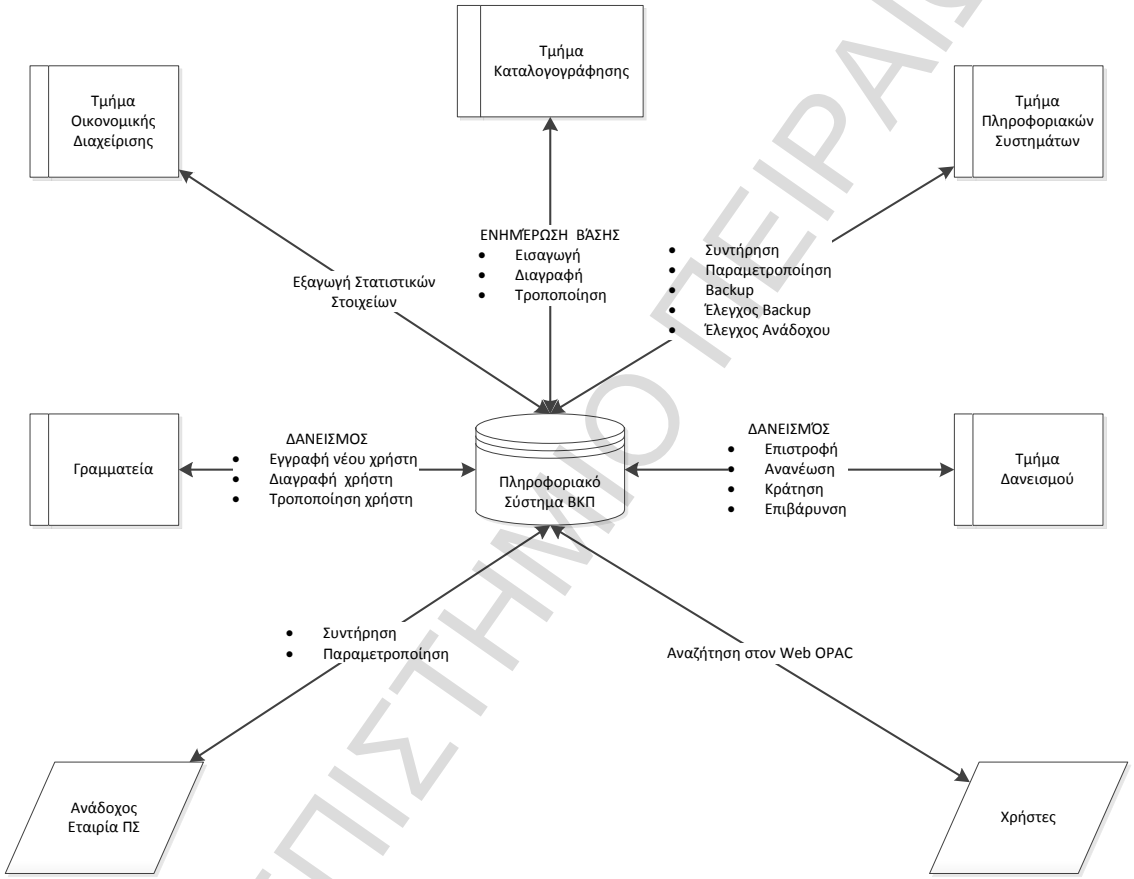


Εικόνα 11. Οργανόγραμμα Βιβλιοθήκης και Κέντρου Πληροφόρησης.

4.1.2 Μελέτη του Συστήματος (Δραστηριότητα 1.2)

Παρουσίαση του Συστήματος

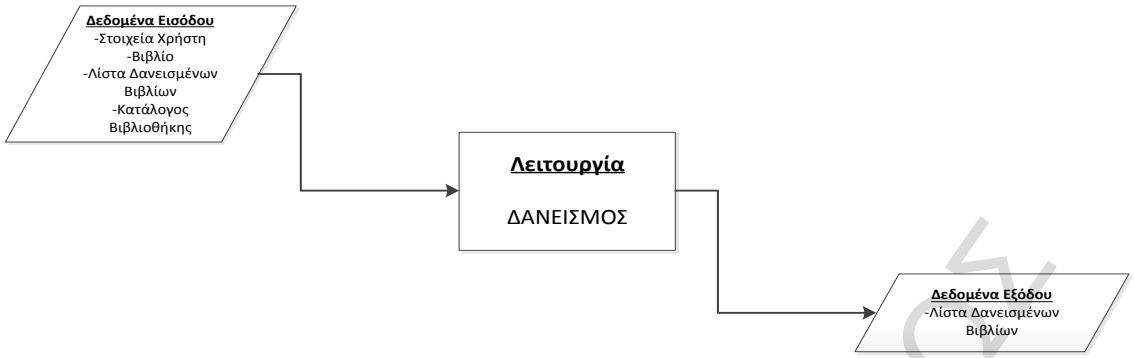
Η λειτουργία της ΒΚΠ σε πολύ μεγάλο βαθμό βασίζεται στο πληροφοριακό σύστημά της και άμεσα γίνεται αντιληπτό ότι αντικείμενο-στόχος της παρούσας μελέτης είναι το σύστημα αυτοματοποίησης της Βιβλιοθήκης HORIZON. Το HORIZON είναι ένα πλήρως ολοκληρωμένο σύστημα βιβλιοθήκης, αρχιτεκτονικής πελάτη/εξυπηρετητή και περιλαμβάνει λειτουργίες όπως η καταλογογράφηση (cataloguing), ο δανεισμός (circulation), οι προσκτήσεις (acquisitions), οι κρατήσεις (holdings), η διαχείριση συστήματος (system administration), online κατάλογο (web OPAC), ευρετηρίαση (indexing).



Εικόνα 12. Το Πληροφοριακό Σύστημα της ΒΚΠ.

Τα ουσιώδη στοιχεία του Συστήματος (essential elements)

Τα ουσιώδη στοιχεία ενός συστήματος σύμφωνα με τη μεθοδολογία [10] διακρίνονται στις **λειτουργίες (functions)** και στην **πληροφορία (information)**για τις οποίες εάν δε διασφαλισθεί η διαθεσιμότητα, η ακεραιότητα και η εμπιστευτικότητα ή κάποιο άλλο κριτήριο ασφάλειας, θα έχει ως αποτέλεσμα τη ζημιά στον οργανισμό. Το ΠΣ της Βιβλιοθήκης ουσιαστικά διακρίνεται σε τέσσερις (4) βασικές λειτουργίες: α) το δανεισμό (συμπεριλαμβάνεται η επιστροφή, ανανέωση, κράτηση, επιβάρυνση, εγγραφή νέου χρήστη, διαγραφή χρήστη, τροποποίηση στοιχείων χρήστη), β) την ενημέρωση της βάσης (διαδικασία καταλογογράφησης), γ) τη συντήρηση-παραμετροποίηση-λήψη αντιγράφων ασφαλείας που γίνεται από το τμήμα πληροφοριακών συστημάτων αλλά και την ανάδοχο εταιρία (IT contractor) και δ) την αναζήτηση στον online κατάλογο της βιβλιοθήκης μέσα από το PORTAL του HORIZON. Για κάθε μία από αυτές τις λειτουργίες ουσιώδη στοιχεία είναι τα δεδομένα εισόδου (information input) και τα δεδομένα εξόδου – αποτελέσματα (information output). Για παράδειγμα, η είσοδος και η έξοδος της διαδικασίας του δανεισμού φαίνεται στο παρακάτω διάγραμμα.



Εικόνα 13. Η λειτουργία του δανεισμού

4.1.3 Προσδιορισμός του στόχου της μελέτης (Δραστηριότητα 1.3)

Κατάλογος Αγαθών-Οντοτήτων (Entities)

Το σύστημα στόχος αποτελείται από ένα σύνολο τεχνικών και μη, **οντοτήτων (entities)**, οι οποίες θα πρέπει να εντοπισθούν και να περιγραφούν. Αυτές οι οντότητες έχουν αδυναμίες τις οποίες μπορούν να εκμεταλλευθούν κάποιες μέθοδοι επίθεσης με συνέπεια να βλάψουν τα ουσιώδη συστατικά του συστήματος στόχου (λειτουργίες και πληροφορία). Αυτές οι οντότητες θα πρέπει να προστατευθούν. Το εργαλείο EBIOS κάνει διαχωρισμό ανάλογα με τον τύπο της κάθε οντότητας και με βάση αυτό το διαχωρισμό έγινε ο καθορισμός των αγαθών του ΠΣ της βιβλιοθήκης.

Λογισμικό (LOG):

- Λειτουργικό σύστημα (LOG_OS): οι εξυπηρετητές του ΠΣ έχουν το Windows Server 2003(E.WSRV) της Microsft, ενώ τα τερματικά – πελάτες τρέχουν Windows XP (E.WXP)
- Πακέτα λογισμικού ή στάνταρ λογισμικό (LOG_STD): χρησιμοποιείται ο jboss web server (E.JBOSS) και η βάση δεδομένων που χρησιμοποιείται είναι η Sybase (E.BASE).
- Εφαρμογή (LOG_APP.1): η διεπαφή του HORIZON που είναι εγκατεστημένη στους η/υ του προσωπικού και παρέχει τη δυνατότητα διαχείρισης της βάσης δεδομένων (E.GUI).

Υλικό (MAT):

- Σταθερός εξοπλισμός (MAT_ACT.2): υπάρχει ένας (1) Web server (E.WEBSRV), (1) Application Server (E.APSRV) , (1) Database Server (E.DBSRV) και ένας (1) Backup Server (E.BUSRV)σε ιεραρχική δομή. Παράλληλα υπάρχουν δύο τερματικά (E.PCCLG, E.PCLOAN) στα οποία είναι εγκατεστημένο το user interface του HORIZON, το ένα χρησιμοποιείται από τους βιβλιοθηκονόμους που κάνουν την ενημέρωση της βάσης και το άλλο από το Τμήμα Δανεισμού (check in, check out, …).

Προσωπικό (PER):

- Ο διαχειριστής συστήματος (PER_EXP): είναι το προσωπικό του τμήματος Πληροφοριακών Συστημάτων(E.SYSA).
- Χρήστες (PER_UTI): είναι οι βιβλιοθηκονόμοι που είναι υπεύθυνοι για την ενημέρωση της βάσης (E.LCTG), οι βιβλιοθηκονόμοι στο τμήμα δανεισμού (E.LLOAN) και οι απλοί χρήστες του online καταλόγου (E.USRS)

Περιβάλλον (PHY):

- Κλιματισμός (PHY_SRV_3): το δωμάτιο στο οποίο είναι εγκατεστημένοι οι εξυπηρετητές διαθέτει κλιματισμό (E.AIR).

Δίκτυο (RES):

- Δίκτυο (RES: Network): το εσωτερικό δίκτυο του πανεπιστημίου (E.NET).

Σύστημα (SYS): Το Web τμήμα του συστήματος (SYS_WEB): Με το Horizon Information Portal ο κατάλογος της βιβλιοθήκης είναι διαθέσιμος στο διαδίκτυο (E.OPAC).

Συσχετισμός Ουσιωδών Στοιχείων – Οντοτήτων

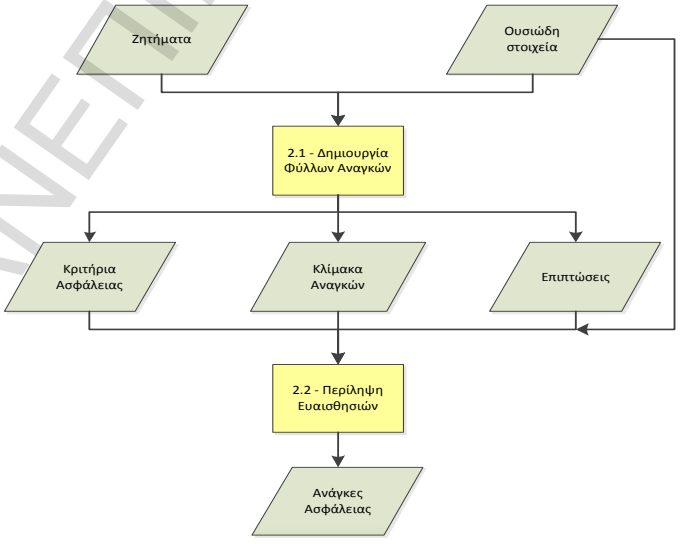
Το πρώτο βήμα ολοκληρώνεται με τη συσχέτιση των ουσιωδών στοιχείων και συγκεκριμένα, α) των σημαντικών λειτουργιών και β) της σημαντικής πληροφορίας που αναλύθηκαν στη δραστηριότητα 1.1.2 με τις οντότητες που συμβάλλουν στην εκτέλεση και επεξεργασία τους αντίστοιχα. Αυτή η συσχέτιση θα χρησιμοποιηθεί κατά τη σύγκριση απειλών και των αναγκών. Αποτέλεσμα αυτού του βήματος είναι η δημιουργία ενός πίνακα στοιχείων-οντοτήτων όπως φαίνεται στη συνέχεια(ολοκληρωμένος ο πίνακας δημιουργήθηκε μέσα από το εργαλείο):

Entities / Elements	H1 E.ASRV	H2 E.BUSRV	H3 E.DBSRV	H4 E.WEBSR	H5 E.PCLOA	H6 E.PCCLG	H7 E.PCUSR	S1 E.WSRV	S2 E.WXP	S3 E.JBOSS	S4 E.BASE	P1 E.SYSA	P2 E.LLOAN	P3 E.LCLG	P4 E.USER	N1 E.NET	S1 E.OPAC
Λειτουργία 1 (Δανεισμός)	x		x		x				x	x			x		x	x	
Λειτουργία 2 Ενημέρωση	x		x			x			x	x	x			x		x	
Πληροφορία1 (Αναζήτηση)							x		x						x	x	x
Πληροφορία2 (Backup)	x	x	x	x				x				x				x	

Πίνακας 8. Πίνακας Ουσιωδών Στοιχείων – Οντοτήτων.

4.2 Βήμα 2 - Έκφραση Αναγκών Ασφάλειας

Το δεύτερο βήμα της μεθοδολογίας συμβάλλει στην εκτίμηση των κινδύνων και στον καθορισμό των κριτηρίων κινδύνου. Επιτρέπει στους χρήστες του συστήματος να εκφράσουν τις ανάγκες για ασφάλεια των λειτουργιών και της πληροφορίας που χειρίζονται. Η έκφραση των αναγκών προκύπτει από τις λειτουργικές απαιτήσεις του συστήματος, ανεξάρτητα από οποιαδήποτε τεχνική λύση. Βασίζεται στην προπαρασκευή και χρήση μίας κλίμακας αναγκών και στον εντοπισμό των επιπτώσεων που ο οργανισμός δεν μπορεί να αποδεχτεί [9]. Η έκφραση αναγκών χρησιμοποιείται επίσης, για τον καθορισμό του τρόπου λειτουργίας του συστήματος, δηλαδή, το γενικό τρόπο διαχείρισης των χρηστών. Αυτό το βήμα διαιρείται σε δύο επιμέρους δραστηριότητες: α) την παραγωγή των φύλλων αναγκών και β) μία περίληψη των ευαισθησιών (**sensitivities**) του συστήματος.



Εικόνα 14. Διάγραμμα ροής της έκφρασης των αναγκών ασφάλειας

4.2.1 Δημιουργία φύλλων Αναγκών (Δραστηριότητα 2.1)

Επιλογή Κριτηρίων Ασφάλειας

Οι ανάγκες ασφάλειας που σχετίζονται με τις σημαντικές λειτουργίες και τη σημαντική πληροφορία εκφράζονται σύμφωνα με τα κριτήρια ασφάλειας [10], τα οποία είναι τα εξής:

- Διαθεσιμότητα (Δ): μία ιδιότητα των ουσιωδών στοιχείων που τους επιτρέπει να έχουν πρόσβαση σε αυτά οι εξουσιοδοτημένοι χρήστες στον απαιτούμενο χρόνο. Για μία λειτουργία αυτό συνεπάγεται ουσιαστικά την εγγύηση της συνέχειας των υπηρεσιών επεξεργασίας και την απουσία προβλημάτων αναφορικά με τους χρόνους απόκρισης. Για μία πληροφορία αυτό συνεπάγεται την εγγύηση της πρόσβασης στα δεδομένα και ότι δεν υπάρχει ολική απώλεια της πληροφορίας (εφόσον υπάρχει διαθέσιμο backup θεωρείται ότι είναι διαθέσιμη).
- Ακεραιότητα (Α): επιτρέπει την ακρίβεια και πληρότητα των ουσιωδών στοιχείων. Για μία λειτουργία εξασφαλίζει ότι ο αλγόριθμος είναι σωστός ή μία αυτοματοποιημένη επεξεργασία εκτελείται σύμφωνα με τις προδιαγραφές και τα αποτελέσματα είναι σωστά και πλήρη. Για μία πληροφορία εγγυάται ότι δεν υπάρχουν λειτουργικά λάθη ή χρήση χωρίς εξουσιοδότηση που να επηρεάζει την ακρίβεια και την πληρότητα των δεδομένων, καθώς και ότι δεν υπάρχει διαφθορά της πληροφορίας.
- Εμπιστευτικότητα (Ε): τα ουσιώδη στοιχεία είναι προσβάσιμα μόνο σε εξουσιοδοτημένους χρήστες. Αυτό για μία λειτουργία σημαίνει προστασία των αλγόριθμων που σχετίζονται με τη διαχείριση κανόνων και αποτελεσμάτων των οποίων η αποκάλυψη σε τρίτους που δεν είναι εξουσιοδοτημένοι είναι επιβλαβής. Για μία πληροφορία σημαίνει μη αποκάλυψη εμπιστευτικών δεδομένων.
- Απόδειξη-λογοδοσία (Accountability): εγγυάται τη μη άρνηση της ευθύνης μίας μεταφοράς ή αποστολής πληροφορίας.
- Ελεγξιμότητα (Auditability): ο έλεγχος για παράδειγμα της μεταφοράς κεφαλαίων χρησιμοποιώντας τα στοιχεία εισόδου.
- Ανωνυμία (Anonymity): ένα μέτρο που καθιστά αδύνατο τον εντοπισμό αυτού που δημιούργησε την πληροφορία (π.χ. ενός ψηφοφόρου).
- Αξιοπιστία (Reliability): συνέπεια μεταξύ της αναμενόμενης συμπεριφοράς και του αποτελέσματος.
- Οποιοδήποτε άλλο κριτήριο ασφάλειας κρίνεται απαραίτητο.

Τα κριτήρια ασφάλειας που επιλέχθηκαν για το πληροφοριακό σύστημα της ΒΚΠ είναι αυτά της διαθεσιμότητας, ακεραιότητας και εμπιστευτικότητας, των σημαντικότερων κριτηρίων στην ασφάλεια πληροφορίας.

Καθορισμός Κλίμακας Αναγκών

Οι ανάγκες ασφάλειας πρέπει να εκφράζονται για κάθε επιλεγμένο κριτήριο. Επίσης, θα πρέπει να ταξινομούνται σε επίπεδα. Για να γίνει αυτό, κάθε επίπεδο αναγκών πρέπει να ορίζεται για κάθε κριτήριο ασφάλειας. Η κλίμακα έχει προεπιλεγμένα πέντε (5) επίπεδα μεταξύ του 0 (καμία παραβίαση) και 4 (πολύ σοβαρή παραβίαση). Στη μελέτη περίπτωσης της ΒΚΠ επιλέξαμε τα εξής τρία επίπεδα:

Ανάγκες Ασφάλειας	**Διαθεσιμότητα**	**Ακεραιότητα**	**Εμπιστευτικότητα**
0	Δεν απαιτείται	Δεν απαιτείται	Δημόσιο
1	Μέτρια	Μέτρια	Περιορισμένης πρόσβασης
2	Υψηλή	Πλήρης	Εμπιστευτικό

Πίνακας 9. Κλίμακα Αναγκών.

Καθορισμός Επιπτώσεων

Σε αυτό το σημείο καθορίζονται οι σημαντικές συνέπειες από κάποια ζημιά στο πληροφοριακό σύστημα. Από τις προτεινόμενες επιπτώσεις (**impacts**) του EBIOS επιλέχθηκαν οι εξής τρείς:

- Διακοπή υπηρεσίας (Interruption of service): αδυναμία παροχής υπηρεσιών από τη ΒΚΠ
- Διατάραξη της εσωτερικής λειτουργίας (Disruption of internal operation): διατάραξη της λειτουργίας της ΒΚΠ και πρόσθετα εσωτερικά κόστη (εργατοώρες, συντήρηση, αναβάθμιση κλπ.)
- Απώλεια εμπιστοσύνης των πελατών (Loss of customer confidence): στην περίπτωση της ΒΚΠ αυτό συνεπάγεται την απώλεια της εμπιστοσύνης της ακαδημαϊκής κοινότητας στις προσφερόμενες υπηρεσίες της βιβλιοθήκης.

Φύλλα Έκφρασης Αναγκών

Από τη στιγμή που θα προσδιοριστούν τα κριτήρια ασφάλειας και οι επιπτώσεις, μπορούμε να συντάξουμε τα φύλλα έκφρασης αναγκών για κάθε σημαντικό στοιχείο. Το EBIOS τα παράγει αυτόματα μόλις ολοκληρώσουμε τα προηγούμενα βήματα.

Blank sensitivities expression sheet

		Impacts			Sensitivity	Comments
Security criterion	Damage	Disturbance of internal operation	Interruption of service	Loss of customer confidence		
Confidentiality	External disclosure					
	Internal disclosure					
	Summary					
Integrity	Accidental modification					
	Deliberate modification					
	Incomplete results					
	Incorrect results					
	Summary					
Availability	Inaccessibility					
	Long interruption					
	Short interruption					
	Total loss (destruction)					
	Summary					

Εικόνα 15. Φύλλο Έκφρασης Αναγκών (Στιγμιότυπο από το EBIOS).

Όπως φαίνεται στην παραπάνω εικόνα έχουν προστεθεί κάποια ζημιογόνα στοιχεία στο κάθε κριτήριο. Στο κριτήριο της εμπιστευτικότητας προστέθηκαν τα ζημιογόνα στοιχεία της εξωτερικής αποκάλυψης (external disclosure) και της εσωτερικής αποκάλυψης (internal disclosure). Στο κριτήριο της ακεραιότητας προστέθηκαν η κατά λάθος τροποποίηση (accidental modification), η εσκεμμένη τροποποίηση (deliberate modification), τα ελλιπή αποτελέσματα (incomplete results) και τα λανθασμένα αποτελέσματα (incorrect results). Στο κριτήριο της διαθεσιμότητας προστέθηκαν τα στοιχεία της μη διαθεσιμότητας (inaccessibility), της μεγάλης διάρκειας διακοπής (long interruption, της μικρής διάρκειας διακοπή (short interruption) και την ολική απώλεια-καταστροφή (total loss-destruction).

4.2.2 Περίληψη των ευαισθησιών (Δραστηριότητα 2.2)

Για τις ανάγκες της μελέτης τα φύλλα έκφρασης αναγκών για το κάθε ουσιώδες στοιχείο (essential element) συμπληρώθηκαν από το διαχειριστή του συστήματος και έναν βιβλιοθηκονόμο. Στην παρακάτω εικόνα (Εικ.16) φαίνεται ο συγκεντρωτικός πίνακας που δημιουργεί μετά τη συμπλήρωση των φύλλων έκφρασης το EBIOS όπου φαίνονται η ευαισθησία του κάθε κριτηρίου για κάθε σημαντική λειτουργία και πληροφορία. Μετά την ολοκλήρωση και του δεύτερου βήματος πρέπει να κάνουμε επικύρωση (validate) για να προχωρήσουμε στα επόμενα στάδια της μεθοδολογίας.

Summarise needs

Summarise sensitivities

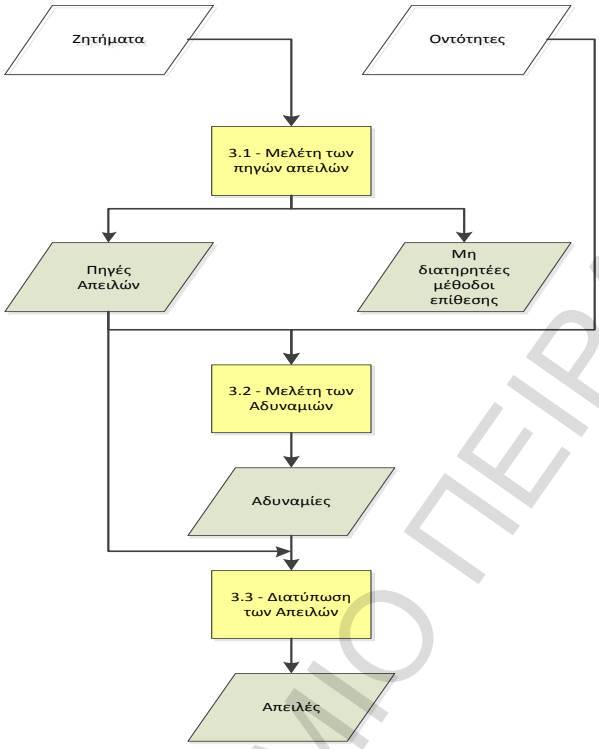
		Persons questioned			Sensitivity	Comments
Essential ele...	Security criteria	Librarian	System Administrator	User		
F.CATG	Availability	2			2	
	Confidentiality	0			0	☑
	Integrity	2			2	☑
F.IT	Availability		2		2	
	Confidentiality		1		1	
	Integrity		2		2	
F.LOAN	Availability	2			2	
	Confidentiality	1			0	
	Integrity	2			2	☑
F.SEARCH	Availability			2	2	
	Confidentiality			0	0	
	Integrity			2	2	
I.BACKUP	Availability		2		1	
	Confidentiality		0		0	☑
	Integrity		2		2	☑
I.BOOK	Availability	2			1	
	Confidentiality	0			0	
	Integrity	2			2	
I.BOOKLIST	Availability	2			1	
	Confidentiality	0			0	
	Integrity	2			2	
I.CATG	Availability	2			2	
	Confidentiality	0			0	
	Integrity	2			2	
I.LIST	Availability	2			1	
	Confidentiality	0			0	
	Integrity	2			1	☑
I.LOG	Availability		2		1	
	Confidentiality		0		1	☑
	Integrity		2		2	☑
I.PARAM	Availability		2			
	Confidentiality		0		1	
	Integrity		2			
I.QUERY	Availability			2	1	
	Confidentiality			0	0	
	Integrity			1	2	
I.RESULT	Availability	2			1	
	Confidentiality	0			0	
	Integrity	1			2	
I.USER	Availability			2	1	
	Confidentiality			2	2	☑

Εικόνα 16. Περίληψη Αναγκών(Στιγμιότυπο από το EBIOS).

4.3 Βήμα 3 - Μελέτη Απειλών

Το τρίτο βήμα της ανάλυσης συμβάλλει επίσης στην εκτίμηση του κινδύνου, μέσα από τον προσδιορισμό των απειλών που επηρεάζουν το σύστημα. Αυτές οι απειλές τυποποιούνται μέσα από τον εντοπισμό των συνιστωσών τους, δηλαδή οι μέθοδοι επίθεσης στις οποίες εκτίθεται ο οργανισμός, οι παράγοντες απειλών που μπορούν να τις χρησιμοποιούν, οι εκμεταλλεύσιμες αδυναμίες των οντοτήτων του συστήματος και το επίπεδο αυτών. Οι απειλές που αναδεικνύονται μέσα από αυτό το

βήμα αφορούν το στοχευμένο σύστημα. Ο χαρακτηρισμός τους είναι ανεξάρτητος των αναγκών ασφάλειας, της επεξεργαζόμενης πληροφορίας και των λειτουργιών που υποστηρίζει το σύστημα [9]. Αυτό το βήμα διαιρείται σε τρεις επιμέρους δραστηριότητες: α) τη μελέτη των πηγών απειλών, β) τη μελέτη των αδυναμιών και γ) την τυποποίηση των απειλών.



Εικόνα 17. Διάγραμμα ροής της μελέτης απειλών.

4.3.1 Μελέτη της προέλευσης των απειλών (Δραστηριότητα 3.1)

Αρχικά επιλέγονται οι μέθοδοι επίθεσης που είναι σχετικές με το στόχο και δικαιολογείται η μη επιλογή των υπόλοιπων μεθόδων. Για τις μεθόδους επίθεσης που απομένουν, θα καθορισθούν τα κριτήρια ασφαλείας που θα μπορούσαν να επηρεαστούν (διαθεσιμότητα, ακεραιότητα, εμπιστευτικότητα) υπό τους όρους του τύπου (φυσική, ανθρώπινη, περιβαλλοντική) και της αιτίας πρόκλησης (ατύχημα, εσκεμμένα). Εάν πρόκειται για ατύχημα, θα πρέπει να αξιολογηθεί η έκθεση και οι διαθέσιμοι πόροι. Εάν είναι εσκεμμένη η επίθεση θα πρέπει να αξιολογηθούν η τεχνογνωσία, οι διαθέσιμοι πόροι και τα κίνητρα.

Κάθε μέθοδος επίθεσης μπορεί να επηρεάσει τουλάχιστον ένα κριτήριο ασφάλειας (Δ,Α,Ε). Γι' αυτό το λόγο όλες οι εναπομείναντες μέθοδοι θα πρέπει να χαρακτηριστούν βάση των κριτηρίων που παραβιάζουν. Οι μέθοδοι επίθεσης χρησιμοποιούνται από τους παράγοντες απειλής (**threat agents**) και γι' αυτόν ακριβώς το λόγο θα πρέπει να χαρακτηρίζονται με βάση αυτούς. Η περιγραφή τους θα πρέπει να περιλαμβάνει τον τύπο και την αιτία πρόκλησης του παράγοντα απειλής. Ο χαρακτηρισμός των παραγόντων απειλής μπορεί να συνοψισθεί σε μία τιμή η οποία θα αναπαριστά την πιθανότητα επίθεσής τους:

- 1 (ατύχημα και τυχαίο γεγονός)
- 2 (περιορισμένες δεξιότητες ή πόροι)
- 3 (υψηλό επίπεδο τεχνογνωσίας, δεξιοτήτων και πόρων)

Αυτή η πιθανότητα επίθεσης μπορεί να χρησιμοποιηθεί για τον καθορισμό ενός κατάλληλου επιπέδου αντοχής των στόχων ασφάλειας. Στον παρακάτω πίνακα παραθέτουμε τις μεθόδους επίθεσης που επιλέξαμε, τα στοιχεία απειλής (τύπος και αιτία), την πιθανότητα επίθεσης και τα κριτήρια ασφαλείας που επηρεάζονται. Οι υπόλοιπες μέθοδοι δεν επιλέχθηκαν είτε διότι κρίθηκε σχεδόν απίθανη η εμφάνισή τους είτε διότι δεν επηρεάζουν το σύστημα της βιβλιοθήκης.

	Μέθοδοι επίθεσης	Στοιχεία απειλής					Πιθανότητα επίθεσης	Διαθεσιμότητα	Ακεραιότητα	Εμπιστευτικότητα
		Τύπος			Αιτία					
		Φυσικός	Ανθρώπινος	Περιβαλλοντικός	Ατύχημα	Εσκεμμένα				
01	Πυρκαγιά	+	+	+	+	+	2	+	+	
05	Καταστροφή εξοπλισμού		+		+	+	1	+	+	
11	Βλάβη κλιματιστικού		+	+	+	+	2	+		
12	Απώλεια παροχής ρεύματος		+	+	+	+	1	+		
13	Βλάβη τηλεπικοινωνιακού εξοπλισμού		+	+	+	+	1	+		
21	Κλοπή εξοπλισμού		+			+		+		+
23	Αποκάλυψη		+		+	+	2			+
24	Δεδομένα από αναξιόπιστες πηγές		+		+	+	3	+	+	
28	Βλάβη εξοπλισμού	+	+		+		1	+		
29	Δυσλειτουργία εξοπλισμού	+	+		+		1	+		
33	Μη εξουσιοδοτημένη χρήση εξοπλισμού		+			+	3	+	+	+
36	Διαφθορά δεδομένων		+			+	3		+	+
41	Άρνηση ενεργειών		+			+	3		+	+
42	Κενό στο διαθέσιμο προσωπικό		+	+	+	+	2	+		

Πίνακας 10. Πίνακας επιλογής και χαρακτηρισμού μεθόδων επίθεσης.

4.3.2 Μελέτη των αδυναμιών (Δραστηριότητα 3.2)

Θα πρέπει να προσδιοριστούν οι ευπάθειες τους συστήματος στόχου, οι οποίες καθιστούν εφικτή την επίθεση, σύμφωνα με τις μεθόδους που επιλέξαμε στην δραστηριότητα 3.1. Μία ευπάθεια είναι ένα χαρακτηριστικό του συστήματος που θα μπορούσε να αξιοποιηθεί από έναν παράγοντα απειλής για να διενεργήσει μία μέθοδο επίθεσης. Αυτό το χαρακτηριστικό, σε συνδυασμό με τις οντότητες του συστήματος, μπορεί να αποτελεί αδυναμία ή ελάττωμα. Για τις παραπάνω μεθόδους επίθεσης που θεωρήσαμε για το πληροφοριακό σύστημα της βιβλιοθήκης, επιλέγουμε τις αδυναμίες των οντοτήτων μέσα από τη λίστα που μας προτείνει η γνωσιακή βάση του EBIOS. Στη συνέχεια παραθέτουμε ενδεικτικά για ορισμένες από τις μεθόδους που αναφέραμε παραπάνω, τις αδυναμίες που εμφανίζονται:

- Για την περίπτωση της <u>πυρκαγιάς</u> διαπιστώσαμε τις εξής αδυναμίες-ευπάθειες: α) ο κλιματισμός που είναι εγκατεστημένος στο δωμάτιο των υπολογιστών (computer room) δε συντηρείται σωστά και β) ανυπαρξία δοκιμών με στόχο τον έλεγχο της αντίδρασης και των διαδικασιών σε περίπτωση ενός τέτοιου συμβάντος.
- Για την μέθοδο <u>καταστροφή εξοπλισμού</u> διαπιστώσαμε τις εξής αδυναμίες: α) έχουν πρόσβαση στον εξοπλισμό και άτομα πλην των ‘ιδιοκτητών’, για παράδειγμα ο υπολογιστής στο τμήμα δανεισμού βρίσκεται σε χώρο από όπου διέρχονται οι φοιτητές με κίνδυνο να προκαλέσουν ζημιά και β) η φυσική πρόσβαση στο γραφείο που βρίσκεται ο υπολογιστής που γίνεται η ενημέρωση της βάσης δεν προστατεύεται, με κίνδυνο να εισέλθει στο χώρο αυτό κάποιος φοιτητής κατά τη διάρκεια απουσίας του προσωπικού.
- Για τη μέθοδο της <u>μη εξουσιοδοτημένης χρήσης του εξοπλισμού</u> παρατηρήθηκε η χρησιμοποίηση του υπολογιστή της ενημέρωσης της βάσης από προσωπικό που δεν ανήκει στο συγκεκριμένο τμήμα.

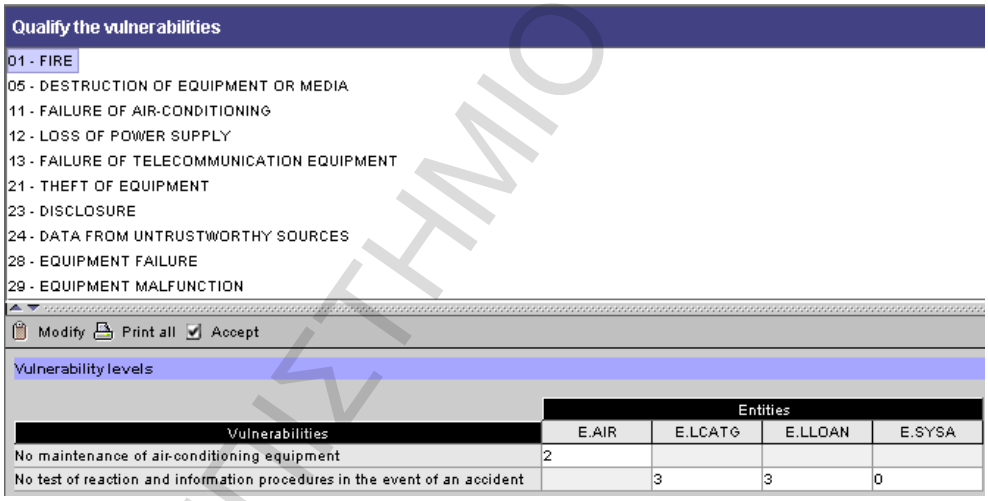
- Για τη μέθοδο δημιουργία κενού στη διαθεσιμότητα του προσωπικού παρατηρήθηκε σε περίπτωση απεργίας να απουσιάζει μεγάλος αριθμός από το προσωπικό, με συνέπεια στη διαθεσιμότητα της παροχής υπηρεσιών της βιβλιοθήκης.

Υπολογισμός του επιπέδου των αδυναμιών

Οι αδυναμίες χαρακτηρίζονται από το επίπεδό τους, το οποίο αντιπροσωπεύει τη δυνατότητα επίτευξης των μεθόδων επίθεσης που μπορούν να τις εκμεταλλευθούν. Το επίπεδο αυτό αξιολογείται βάση των εξής κριτηρίων: α) σε σχέση με το ειδικό περιβάλλον του συστήματος και β) σε σχέση με την εξέλιξη της τεχνολογίας στο συγκεκριμένο τομέα. Σκοπός του υπολογισμού του επιπέδου των αδυναμιών είναι η διασφάλιση ότι μόνο οι σχετικές αδυναμίες παραμένουν και εν συνεχεία η ιεράρχησή του βάση προτεραιότητας. Η κλίμακα η οποία προτείνεται από το EBIOS και που χρησιμοποιήσαμε στην περίπτωσή μας είναι η εξής:

0	Εντελώς απίθανο ή ανέφικτο
1	Χαμηλή πιθανότητα ή απαιτούνται πολύ σημαντικοί πόροι και/ή πολύ υψηλό επίπεδο γνώσεων στο συγκεκριμένο τομέα
2	Μέτρια πιθανότητα ή απαιτείται κάποιος βαθμός εμπειρίας ή/και ειδικός εξοπλισμός
3	Υψηλή πιθανότητα ή δυνατή με τη χρήση τυποποιημένων μέσων ή/και βασικών γνώσεων
4	Βέβαιο ή εφικτό για τον καθένα

Πίνακας 11. Πίνακας κλίμακας των αδυναμιών.



Εικόνα 18. Επίπεδα αδυναμιών (Στιγμιότυπο από το EBIOS).

4.3.3 Διατύπωση των απειλών (Δραστηριότητα 3.3)

Η διατύπωση των απειλών δεν περιέχει ένα σταθερό όγκο πληροφορίας. Το βασικό σημείο στη συγκεκριμένη δραστηριότητα είναι η διατύπωση μίας απειλής να εκφράζει ένα σενάριο επίθεσης με τρόπο ρητό και λεπτομερή ανάλογα με το σκοπό της μελέτης. Ιδανικά η διατύπωση μίας απειλής θα πρέπει να περιέχει: α) τον παράγοντα απειλής με τα χαρακτηριστικά του και την πιθανότητα επίθεσης, β) τη μέθοδο επίθεσης από τον παράγοντα απειλής και τα κριτήρια ασφάλειας που επηρεάζονται, γ) τις εκμεταλλεύσιμες αδυναμίες και τα επίπεδά αυτών, δ) τις οντότητες που επηρεάζουν οι αδυναμίες αυτές. Οι απειλές δύναται να χαρακτηριστούν από μία τιμή ευκαιρίας (**opportunity value**) η οποία καθορίζεται σύμφωνα με το επίπεδο των αδυναμιών. Παρόλο που είναι υποκειμενικές, έχουν το πλεονέκτημα να είναι αλληλένδετες τιμές. Ενδεικτικά, αναφέρουμε τις διατυπώσεις ορισμένων απειλών (σε παρένθεση είναι ο τίτλος που δώσαμε στην αντίστοιχη απειλή στο EBIOS):

- Πυρκαγιά: α) Οι συνέπειες μίας τυχαίας πυρκαγιάς (λόγω κεραυνών ή ενός βραχυκυκλώματος ή μίας ανάφλεξης) επιδεινώνεται από την μη σωστή συντήρηση του

κλιματισμού στο δωμάτιο υπολογιστών (M.INCINDENT-AIR), β) τα αποτελέσματα μίας ακούσιας ή εκούσιας πυρκαγιάς επιδεινώνονται λόγω της απουσίας διαδικαστικών δοκιμών για τη διαπίστωση της αντίδρασης και της έλλειψης εξοικείωσης με τα μέτρα ασφάλειας εκ μέρους του προσωπικού (M.INCIDENT-PER).

- Κενό στη διαθεσιμότητα του προσωπικού: η απειλή της δημιουργίας κενού στη διαθεσιμότητα του προσωπικού επιδεινώνεται α) από την έλλειψη ενός ενημερωτικού και εκπαιδευτικού προγράμματος που αφορά τις διαδικασίες που σχετίζονται με τη συνέχεια των επαγγελματικών δραστηριοτήτων ή την έλλειψη διαδικασιών για τη διαχείριση της συνέχειας των επαγγελματικών δραστηριοτήτων του οργανισμού ή την έλλειψη διαδικασιών για μεταφορά της γνώσης (M.DISPO-ORGA) και β) από την έλλειψη προσωπικού εξαιτίας μίας ασθένειας ή λόγω απουσίας του (M.DISPO-PER).

Αποτέλεσμα της παραπάνω διαδικασίας είναι η δημιουργία μίας λίστας με όλες τις απειλές που αντιμετωπίζει το πληροφοριακό μας σύστημα, οι οποίες μπορούν να ταξινομηθούν κατά φθίνουσα σειρά ανάλογα με τις ευκαιρίες απειλής. Πρόκειται για ένα εργαλείο επικοινωνίας το οποίο πρέπει να λάβει ιδιαίτερη προσοχή, διότι παρέχει την πιο σαφή έκφραση αυτών στα οποία ο οργανισμός είναι εκτεθειμένος. Οι απειλές με το υψηλότερο επίπεδο δυνατότητας θα πρέπει να εμφανίζονται στην κορυφή της λίστας ώστε οι ενδιαφερόμενοι να έχουν πλήρη επίγνωση. Στην παρακάτω εικόνα φαίνεται η λίστα με τις απειλές όπως τη δημιούργησε το EBIOS, με τις απειλές να είναι ταξινομημένες με βάση τη δυνατότητά (opportunity) τους.

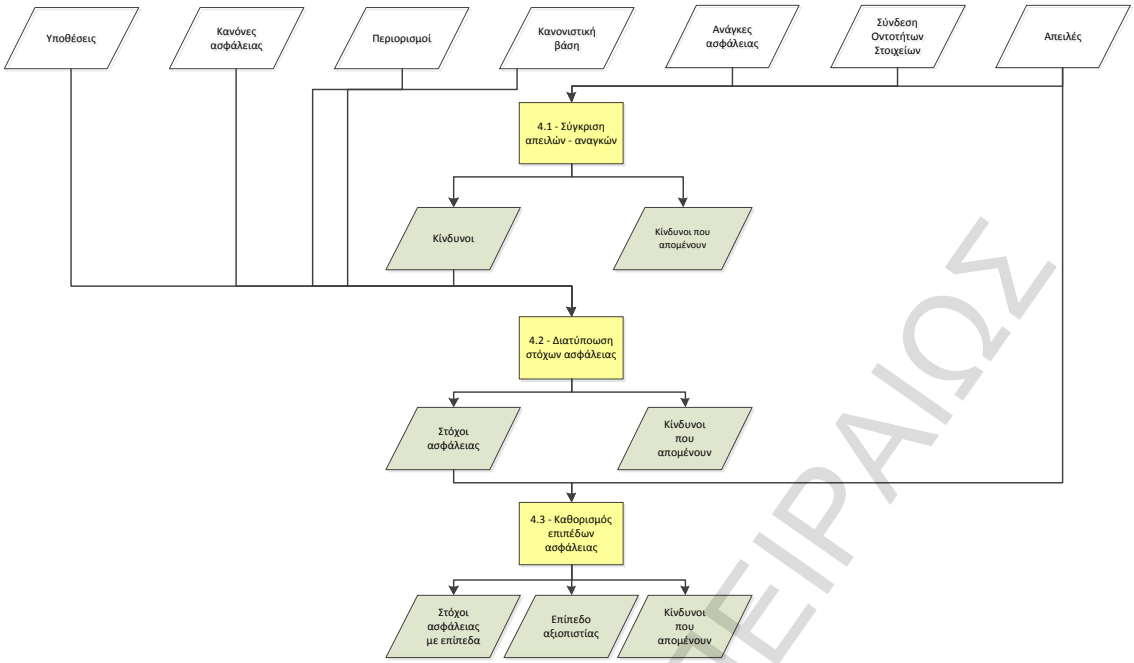
Summarise the threats

Threats	Security criteria			Opportunity	Attack potential
	Availability	Confidentiality	Integrity		
M.AUTH-SHAR	☑	☑	☑	4	3
M.COR-REMOT	☐	☑	☑	4	3
M.DEN-REMOT	☐	☐	☑	4	3
M.UNAUT-INST	☑	☑	☑	4	3
M.DATA-UPD	☑	☐	☑	4	3
M.COR-PSW	☐	☑	☑	4	3
M.AIR-MAT-MAIN	☑	☐	☐	4	2
M.DISPO-PER	☑	☐	☐	4	2
M.DISPO-ORGA	☑	☐	☐	4	2
M.FAIL-MAIN	☑	☐	☐	4	1
M.DATA-UNTR	☑	☐	☑	3	3
M.UNAUT-AWAR	☑	☑	☑	3	3
M.DEN-AUDIT	☐	☐	☑	3	3
M.INCIDENT-PER	☑	☐	☑	3	2
M.DIV-LOG	☐	☑	☐	3	2
M.DESTR-MAT-PER	☑	☐	☑	3	1
M.TELECOM-PHY	☑	☐	☐	3	1
M.MAL-EQUI	☑	☐	☐	3	1
M.TELECOM-ORGA	☑	☐	☐	3	1
M.DEN-PASS	☐	☐	☑	2	3
M.INCIDENT-AIR	☑	☐	☑	2	2
M.DESTR-MAT-PHY	☑	☐	☑	2	1

Εικόνα 19 Συνοπτικός Πίνακας (Στιγμιότυπο από EBIOS).

4.4 Βήμα 4 - Προσδιορισμός στόχων ασφάλειας

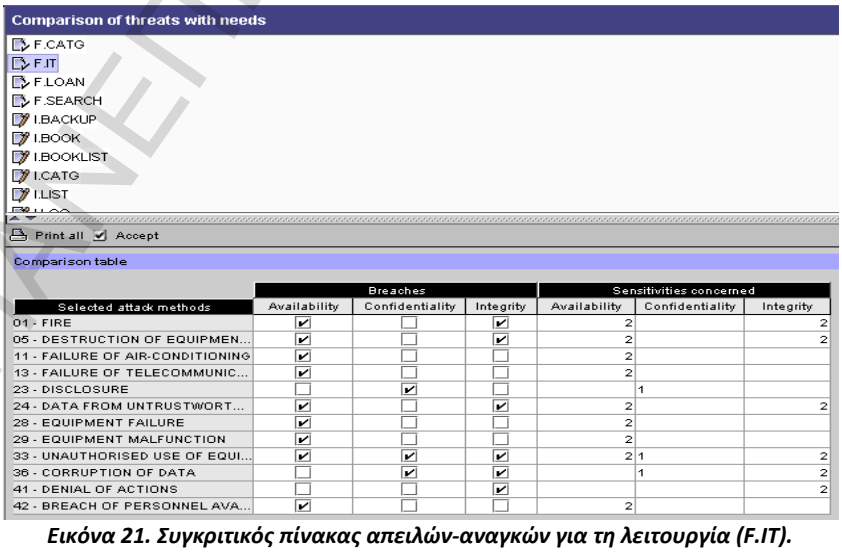
Στο βήμα 4 της μεθοδολογίας γίνεται η αξιολόγηση και η αντιμετώπιση των κινδύνων που επηρεάζουν το σύστημα. Η σύγκριση των απειλών με τις ανάγκες ασφάλειας θα πρέπει να υπογραμμίζει τους κινδύνους που θα πρέπει να καλύπτονται από τους στόχους ασφάλειας(**security objectives**). Αυτοί οι στόχοι αποτελούν τις προδιαγραφές ασφάλειας του συστήματος στόχου και του περιβάλλοντος. Θα πρέπει να είναι σύμφωνοι με το σύνολο των υποθέσεων, περιορισμών, κανονισμών και κανόνων ασφάλειας που προσδιορίστηκαν στο βήμα 1. Σε αυτό το βήμα προσδιορίζονται επίσης τα επίπεδα των στόχων ασφάλειας και αξιπιστίας (**assurance level**) [9]. Το βήμα αυτό διαιρείται σε τρεις επιμέρους δραστηριότητες: α) σύγκριση απειλών-αναγκών, β) Διατύπωση των στόχων ασφάλειας και γ) καθορισμός των επιπέδων ασφάλειας.



Εικόνα 20. Διάγραμμα ροής του Προσδιορισμού των στόχων ασφάλειας.

4.4.1 Σύγκριση απειλών – αναγκών (Δραστηριότητα 4.1)

Για τον προσδιορισμό των κινδύνων που αντιμετωπίζει ένας οργανισμός, θα πρέπει να επισημανθούν τα βασικά στοιχεία που επηρεάζονται από τις απειλές. Αυτό επιτυγχάνεται από τη σύγκριση των απειλών που προσδιορίσθηκαν στο βήμα 3 με τις ανάγκες ασφαλείας που προσδιορίσθηκαν στο βήμα 2. Οι ανάγκες έχουν εκφραστεί σύμφωνα με τα τρία κριτήρια Δ,Α,Ε και αντίστοιχα οι απειλές έχουν χαρακτηρισθεί σε σχέση με αυτά τα κριτήρια. Τώρα, το κάθε ουσιώδες στοιχείο θα πρέπει να συγκριθεί με κάθε απειλή, προκειμένου να καθορισθούν οι ενδεχόμενες συνέπειες από την εμφάνισή της. Το EBIOS παράγει έναν πίνακα για κάθε ένα ουσιώδες στοιχείο. Από τις επιλεγμένες μεθόδους επίθεσης, κρατούνται μόνο εκείνες οι οποίες είναι ικανές να εκμεταλλευθούν τις αδυναμίες του συγκεκριμένου στοιχείου. Αυτό ελέγχεται μέσα από τον πίνακα συσχέτισης οντοτήτων – στοιχείων που παράχθηκε στο βήμα 1. Στην εικόνα 21 φαίνεται ο πίνακας που δημιουργήθηκε από το EBIOS τη λειτουργία της συντήρησης – παραμετροποίησης – λήψης αντιγράφων ασφαλείας (F.IT) του πληροφοριακού συστήματος της ΒΚΠ.



Selected attack methods	Breaches			Sensitivities concerned		
	Availability	Confidentiality	Integrity	Availability	Confidentiality	Integrity
01 - FIRE	☑	☐	☑	2		2
05 - DESTRUCTION OF EQUIPMEN...	☑	☐	☑	2		2
11 - FAILURE OF AIR-CONDITIONING	☑	☐	☐	2		
13 - FAILURE OF TELECOMMUNIC...	☑	☐	☐	2		
23 - DISCLOSURE	☐	☑	☐		1	
24 - DATA FROM UNTRUSTWORT...	☑	☐	☑	2		2
28 - EQUIPMENT FAILURE	☑	☐	☐	2		
29 - EQUIPMENT MALFUNCTION	☑	☐	☐	2		
33 - UNAUTHORISED USE OF EQUI...	☑	☑	☑	2	1	2
36 - CORRUPTION OF DATA	☐	☑	☑		1	2
41 - DENIAL OF ACTIONS	☐	☐	☑			2
42 - BREACH OF PERSONNEL AVA...	☑	☐	☐	2		

Εικόνα 21. Συγκριτικός πίνακας απειλών-αναγκών για τη λειτουργία (F.IT).

Στόχος είναι να καθορισθούν οι κίνδυνοι παραβίασης των αναγκών ασφάλειας των ουσιωδών στοιχείων από την υλοποίηση μίας απειλής. Το EBIOS συνοψίζει όλους τους παραπάνω πίνακες σε έναν συγκεντρωτικό πινάκα, ο οποίος παρέχει μία συνολική εικόνα των κινδύνων. Στην παρακάτω εικόνα φαίνεται ο συγκεντρωτικός πίνακας που δημιούργησε το EBIOS για το πληροφοριακό σύστημα της ΒΚΠ.

Sensitivities concerned by the threats

		Essential elements													
Threats	Security criteria	F.CATG	F.IT	F.LOAN	F.SEARCH	I.BACKUP	I.BOOK	I.BOOKLIST	I.CATG	I.LIST	I.LOG	I.PARAM	I.QUERY	I.RESULT	I.USER
M.AIR-MAT-...	Availability	2	2	2		1	1	1	2	1	1			1	1
	Confidentiality														
	Integrity														
M.AUTH-SHAR	Availability	2	2	2	2	1	1	1	2	1	1		1	1	1
	Confidentiality	0	1	0	0	0	0	0	0	0	1	1	0	0	2
	Integrity	2	2	2	2	2	2	2	2	1	2		2	2	2
M.COR-PSW	Availability														
	Confidentiality	0	1	0	0	0	0	0	0	0	1	1	0	0	2
	Integrity	2	2	2	2	2	2	2	2	1	2		2	2	2
M.COR-REM...	Availability														
	Confidentiality	0	1	0	0	0	0	0	0	0	1	1	0	0	2
	Integrity	2	2	2	2	2	2	2	2	1	2		2	2	2
M.DATA-UNTR	Availability	2	2	2	2	1		1	2		1		1	1	1
	Confidentiality														
	Integrity	2	2	2	2	2		2	2		2		2	2	2
M.DATA-UPD	Availability	2	2	2	2	1		1	2		1		1	1	1
	Confidentiality														
	Integrity	2	2	2	2	2		2	2		2		2	2	2
M.DEN-AUDIT	Availability														
	Confidentiality														
	Integrity	2	2	2	2	2	2	2	2	1	2		2	2	2
M.DEN-PASS	Availability														
	Confidentiality														
	Integrity	2	2	2	2	2	2	2	2	1	2		2	2	2
M.DEN-REMOT	Availability														
	Confidentiality														
	Integrity	2	2	2	2	2	2	2	2	1	2		2	2	2
M.DESTR-M...	Availability	2	2	2			1	1	2	1					1
	Confidentiality														
	Integrity	2	2	2			2	2	2	1					2
M.DESTR-M...	Availability	2	2	2			1	1	2	1					1
	Confidentiality														
	Integrity	2	2	2			2	2	2	1					2
M.DISPO-OR...	Availability	2	2	2		1	1	1		1	1				
	Confidentiality														
	Integrity														
M.DISPO-PER	Availability	2	2	2		1	1	1		1	1				
	Confidentiality														
	Integrity														
M.DIV-LOG	Availability														
	Confidentiality	0	1	0		0	0	0		0	1				
	Integrity														
M.FAIL-MAIN	Availability	2	2	2		1	1	1	2	1	1			1	1
	Confidentiality														

Εικόνα 22. Συγκεντρωτικός πίνακας κινδύνων.

Διατύπωση και Ταξινόμηση των κινδύνων

Με βάση τον συγκεντρωτικό πίνακα, τη διατύπωση των απειλών και την κλίμακα αναγκών, θα πρέπει να διατυπωθούν με ξεκάθαρο τρόπο οι κίνδυνοι. Το πόσο λεπτομερής θα είναι η διατύπωση εξαρτάται από την απαιτούμενη ανάλυση. Στην καλύτερη περίπτωση, η διατύπωση των κινδύνων θα πρέπει να περιλαμβάνει τον παράγοντα απειλής, τη μέθοδο επίθεσης, τις αδυναμίες που εκμεταλλεύεται, τις οντότητες που παρουσιάζουν αυτές τις αδυναμίες, την πιθανότητα απειλής, τις κύριες ανάγκες ασφάλειας που απαιτούνται και τις επιπτώσεις στον οργανισμό.

Ο κατάλογος των κινδύνων που προκύπτει μπορεί να ταξινομηθεί κατά φθίνουσα σειρά των μέγιστων τιμών των αναγκών ασφάλειας και κατά φθίνουσα σειρά των ευκαιριών (**opportunity**) εμφάνισης των απειλών. Ο κατάλογος αυτός παρέχει μια σαφέστερη διατύπωση των πραγματικών κινδύνων που αντιμετωπίζει ο οργανισμός. Οι κίνδυνοι που θα μπορούσαν να επηρεάσουν τις πιο σημαντικές ανάγκες ασφαλείας εμφανίζονται στην κορυφή της λίστας, ώστε οι ενδιαφερόμενοι να έχουν πλήρη επίγνωση και εν συνεχεία να αντιμετωπίζονται ως προτεραιότητες. Στην εικόνα 23 φαίνεται ο πίνακας που δημιούργησε το EBIOS και ταξινομεί τους κινδύνους με βάση τα κριτήρια ασφαλείας και την ευκαιρία εμφάνισης.

4.4.2 Διατύπωση των στόχων ασφάλειας

Οι στόχοι ασφάλειας θα πρέπει να καλύπτουν όλους τους παραπάνω κινδύνους, λαμβάνοντας υπόψη τις υποθέσεις, τους κανόνες ασφάλειας και κυρίως τους περιορισμούς και τους ισχύοντες κανονισμούς που προσδιορισθήκαν στο βήμα1. Επίσης, θα πρέπει να είναι σύμφωνοι με τους λειτουργικούς στόχους του συστήματος και το φυσικό περιβάλλον. Οι στόχοι ασφάλειας θα πρέπει να καλύπτουν τα εξής στοιχεία του κινδύνου: α) τις πηγές απειλής (μέθοδοι επίθεσης και παράγοντες απειλής), β) τις

εκμεταλλεύσιμες αδυναμίες και γ) τις συνέπειες (ουσιώδη στοιχεία που επηρεάζονται και επιπτώσεις στον οργανισμό. Στον πίνακα 12 παρουσιάζονται ενδεικτικά ορισμένοι από τους στόχους ασφαλείας που επιλέχθηκαν από τη γνωσιακή βάση του EBIOS.

Summarise sensitivities

Risks	Security criteria	Opportunity
R.AIR-MAT-MAIN	2	4
R.AUTH-SHAR	2	4
R.COR-PSW	2	4
R.COR-REMOT	2	4
R.UNAUT-INST	2	4
R.DATA-UPD	2	4
R.DEN-REMOT	2	4
R.DISPO-ORGA	2	4
R.DISPO-PER	2	4
R.FAIL-MAIN	2	4
R.DATA-UNTR	2	3
R.UNAUT-AWAR	2	3
R.DEN-AUDIT	2	3
R.DESTR-MAT-PER	2	3
R.INCIDENT-PER	2	3
R.MAL-EQUI	2	3
R.TELECOM-ORGA	2	3
R.TELECOM-PHY	2	3
R.DEN-PASS	2	2
R.INCIDENT-AIR	2	2
R.DESTR-MAT-PHY	2	2
R.DIV-LOG	1	3

Εικόνα 23. Ταξινόμηση των Κινδύνων.

O.MAT_03	Μέτριες αλλαγές στο περιβάλλον (θερμοκρασία, υγρασία, κλιματισμός) δε θα πρέπει να οδηγούν σε ανώμαλη συμπεριφορά του ηλεκτρονικού εξοπλισμού και λοιπών μέσων.
O.LOG_03	Όλες οι ενημερώσεις του λογισμικού θα πρέπει να είναι αναγνωρίσιμες και αιτιολογημένες
O.LOG_08	Ο οργανισμός πρέπει να ελέγχει τη λίστα με τις εγκατεστημένες διαμορφώσεις (configuration) στον εξοπλισμό και να εγγυάται τη συμμόρφωσή τους στο χρόνο.
O.ORG_10	Θα πρέπει να διασφαλίζεται ότι χρησιμοποιούνται ισχυροί κωδικοί πρόσβασης από τους χρήστες και γίνεται σωστή διαχείριση αυτών
O.RES_06	Θα πρέπει να σχεδιάζεται και ελέγχεται η πρόσβαση στο δίκτυο
O.ORG_06	Η πολιτική για την προστασία από ιούς πρέπει να αποτρέπει την είσοδο και εξάπλωση οποιουδήποτε κακόβουλου λογισμικού στο σύστημα
O.ORG_27	Θα πρέπει να ελέγχεται ότι όλο το υλικό και λογισμικό συντηρείται κατάλληλα.

Πίνακας 12. Στόχοι ασφαλείας.

Σκοπός των παραπάνω στόχων είναι η αντιμετώπιση και ελαχιστοποίηση των κινδύνων που απειλούν το σύστημα στόχο λαμβάνοντας υπόψη τις υποθέσεις και τους κανόνες ασφάλειας. Κατόπιν, θα πρέπει να ελεγχθεί το κατά πόσο είναι απαραίτητοι και κατάλληλοι αυτοί οι στόχοι., δηλαδή θα πρέπει να αποδειχθεί ότι αυτοί οι στόχοι α)καλύπτουν επαρκώς όλους τους κινδύνους β) καλύπτουν επαρκώς τους κανόνες ασφάλειας και γ) είναι σχετικοί με τις υποθέσεις και τα ζητήματα που διακυβεύονται για το σύστημα. Η κάλυψη μπορεί να αντικατασταθεί από μία τιμή: 0 για καμία κάλυψη, 1 για μερική κάλυψη και 2 για πλήρη κάλυψη. Τέλος, θα πρέπει να παρουσιασθεί ότι κάθε στόχος ασφάλειας αποτελεί μέσο αντίδρασης για τουλάχιστον ένα κίνδυνο, ένα κανόνα ασφάλειας, μία υπόθεση ή έναν περιορισμό. Στην εικόνα 24 φαίνεται σε ποιους κινδύνους, περιορισμούς και κανονισμούς αντιστοιχεί ο κάθε στόχος ασφάλειας και ο βαθμός κάλυψης μέσα από το περιβάλλον του EBIOS.

4.4.3 Καθορισμός επιπέδων ασφάλειας (Δραστηριότητα 4.3)

Προσδιορισμός επιπέδου δυναμικότητας των στόχων ασφάλειας

Το EBIOS θεωρεί τρία επίπεδα δυναμικότητας των μέτρων ασφάλειας, σύμφωνα και με τον ορισμό της δυναμικότητας των λειτουργικών επιπέδων που προτείνεται στο ISO/IES 15408 (Information technology-Security techniques-Evaluation criteria for IT security), εκφράζοντας την ελάχιστη προσπάθεια που απαιτείται για τη διακοπή μίας συμπεριφοράς ασφάλειας από μία άμεση επίθεση:

1. **Βασικό επίπεδο**: παρέχει επαρκή προστασία απέναντι σε μία τυχαία παραβίαση της ασφάλειας του συστήματος από χαμηλής δυναμικότητας εισβολείς.
2. **Μεσαίο επίπεδο**: παρέχει επαρκή προστασία απέναντι σε απλής υλοποίησης ή εσκεμμένες παραβιάσεις ασφάλειας του συστήματος από μέτριας δυναμικότητας εισβολείς.
3. **Υψηλό επίπεδο**: παρέχει επαρκή προστασία απέναντι σε σχεδιασμένες και οργανωμένες παραβιάσεις του συστήματος από υψηλής δυναμικότητας εισβολείς.

Επιλογή επιπέδου απαιτήσεων για αξιοπιστία

Το EBIOS προτείνει επτά (7) προκαθορισμένα επίπεδα αξιοπιστίας (assurance levels) γνωστά ως Επίπεδα Εκτίμησης Διασφάλισης (EAL – Evaluation Assurance Levels):

EAL 1 – Λειτουργική Δοκιμή

EAL 2 – Οργανωτική Δοκιμή

EAL 3 – Δοκιμή και έλεγχος μεθοδολογίας

EAL 4 – Σχεδιασμός, έλεγχος και αξιολόγηση μεθοδολογίας

EAL 5 – Ημι-επίσημος σχεδιασμός και δοκιμή

EAL 6 – Ημι-επίσημος έλεγχος σχεδιασμού και δοκιμή

EAL 7 – Επίσημος έλεγχος σχεδιασμού και δοκιμή

Το Επίπεδο Εκτίμησης Διασφάλισης αντιπροσωπεύει την εμπιστοσύνη στην υλοποίηση των στόχων ασφάλειας. Όσο υψηλότερο επίπεδο επιλέξουμε τόσο μεγαλύτερη θα είναι η εγγύηση του οργανισμού απέναντι στις λειτουργικές απαιτήσεις. Ωστόσο, θα πρέπει να συνυπολογισθεί και το κόστος εφαρμογής τους, καθώς επίσης και η σκοπιμότητά τους για τον οργανισμό. Στην περίπτωσή μας επιλέξαμε το πρώτο επίπεδο ασφάλισης EAL 1.

Coverage table

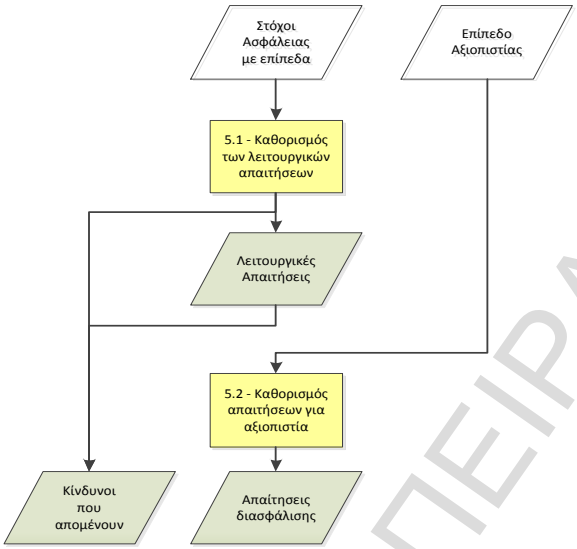
Type	Title	O.LOG_03	O.LOG_08	O.LOG_11	O.LOG_12	O.LOG_13	O.MAT_03	O.MAT_07	O.MAT_10	O.MAT_14	O.ORG_01	O.RES_06	O.TEST	ORG_13	PER_13	ORG_22	Coverage
Risks	R.AIR-MAT-M...						✔						✔				2
	R.AUTH-SHAR				✔												1
	R.COR-PSW																2
	R.COR-REMOT			✔								✔					2
	R.DATA-UNTR		✔														1
	R.DATA-UPD	✔	✔														2
	R.DEN-AUDIT															✔	2
	R.DEN-PASS																2
	R.DEN-REMOT			✔								✔					1
	R.DESTR-MA...																2
	R.DESTR-MA...																1
	R.DISPO-OR...																2
	R.DISPO-PER																2
	R.DIV-LOG																1
	R.FAIL-MAIN									✔							2
	R.INCIDENT-...												✔				2
	R.INCIDENT-...																2
	R.MAL-EQUI									✔				✔			2
	R.TELECOM-...												✔				2
	R.TELECOM-...												✔				1
	R.UNAUT-AW...																2
	R.UNAUT-INST		✔														2
General const...	C.BUDGET	✔															1
	C.CLEANING							✔			✔						2
	C.INVEST														✔		2
	C.TEMP																1
	C.TIME																1
Regulatory o...	Compliance ...																2
Security oper...	Multilevel			✔		✔			✔		✔						2

Εικόνα 24. Συγκεντρωτικός πίνακας στόχων ασφάλειας.

4.4 Καθορισμός Απαιτήσεων Ασφάλειας

Στο βήμα 5 της μεθοδολογίας καθορίζεται ο τρόπος επίτευξης των στόχων ασφάλειας, δηλαδή πως πρέπει να αντιμετωπιστούν οι κίνδυνοι που επηρεάζουν το σύστημα [9]. Γι' αυτό το λόγο απαιτείται ο καθορισμός α) των λειτουργικών απαιτήσεων ασφάλειας που περιγράφουν την απαιτούμενη συμπεριφορά που ορίστηκε στο προηγούμενο βήμα και β) των απαιτήσεων για αξιοπιστία. Οι απαιτήσεις αυτές καταρτίσθηκαν σύμφωνα με τις λειτουργικές απαιτήσεις και απαιτήσεις για

αξιοπιστία που προτείνονται από το ISO 15408 (Κοινά Κριτήρια-Common Criteria). Η κάλυψη των στόχων ασφάλειας θα πρέπει να αιτιολογείται από μία λογική που αποδεικνύει την αναγκαιότητα και επάρκειά τους. Το βήμα αυτό διαιρείται σε δύο επιμέρους δραστηριότητες: α) τον καθορισμό των λειτουργικών απαιτήσεων και β) τον καθορισμό των απαιτήσεων για αξιοπιστία.



Εικόνα 25. Διάγραμμα ροής του καθορισμού των απαιτήσεων ασφάλειας.

4.5.1 Καθορισμός λειτουργικών απαιτήσεων ασφάλειας (Δραστηριότητα 5.1)

Οι λειτουργικές απαιτήσεις ασφάλειας αντιπροσωπεύουν το μέσο για την επίτευξη των στόχων ασφάλειας και συνεπώς, για τη θεραπεία των σχετικών κινδύνων. Οι λειτουργικές απαιτήσεις συμβάλλουν όχι μόνο στη μείωση των κινδύνων, αλλά στην απόρριψη, τη μεταφορά τους ή την παραδοχή τους. Η απόρριψη ενός κινδύνου θα οδηγήσει στην τροποποίηση της δομής του συστήματος στόχου για να εξαλειφθεί η έκθεσή του σε αυτόν. Η μεταφορά ενός κινδύνου θα οδηγήσει στη λήψη συγκεκριμένων μέτρων όπως, η υπογραφή μίας ασφαλιστικής σύμβασης. Η παραδοχή ενός κινδύνου θα έχει ως αποτέλεσμα την ανυπαρξία κάποιας λειτουργικής απαίτησης και θα γίνει αποδεκτό ότι οι στόχοι ασφάλειας δεν ικανοποιούνται πλήρως. Στον παρακάτω πίνακα παρουσιάζονται οι κύριοι τύποι μέτρων ασφάλειας που ορίζονται από τις λειτουργικές απαιτήσεις σε σχέση με τα συστατικά του κινδύνου.

	Κύρια συστατικά κινδύνου		
Κύριοι τύποι μέτρων	Αδυναμίες-Ευπάθειες	Πηγές απειλών	Συνέπειες
Πρόβλεψη και προετοιμασία	X	X	X
Αποτροπή		X	
Προστασία	X		
Εντοπισμός	X	X	
Περιορισμός		X	X
Καταπολέμηση	X		X
Ανάκτηση			X
Αποκατάσταση			X
Αποζημίωση			X

Πίνακας 13. Κύριοι τύποι μέτρων ασφάλειας.

Το EBIOS χρησιμοποιεί τη λίστα λειτουργικών απαιτήσεων των Κοινών Κριτηρίων (Common Criteria) η οποία αποτελείται από κλάσεις, οικογένειες και λειτουργικά στοιχεία. Είναι πιθανό να υπάρχουν εξαρτήσεις μεταξύ των λειτουργικών στοιχείων, που εμφανίζονται στην περίπτωση που ένα στοιχείο δεν είναι αυτάρκες και η παρουσία του εξαρτάται από την παρουσία ενός άλλου. Επίσης, είναι πιθανόν

να υπάρχουν εξαρτήσεις και μεταξύ των λειτουργικών στοιχείων και στοιχείων διασφάλισης (assurance). Το EBIOS προσφέρει τη δυνατότητα προσθήκης λειτουργικών απαιτήσεων σε περίπτωση που δεν αρκούν αυτές που περιλαμβάνονται στη γνωσιακή βάση. Στην καλύτερη περίπτωση η διατύπωση μίας λειτουργικής απαίτησης θα πρέπει να είναι **ειδική, μετρήσιμη, εφικτή, ρεαλιστική και καθορισμένου χρόνου.**

Τέλος, θα πρέπει να δημιουργηθεί ένα πλέγμα κάλυψης, για τη διαβεβαίωση ότι όλοι οι στόχοι ασφάλειας που αφορούν το σύστημα ή το περιβάλλον του καλύπτονται από μία τουλάχιστον λειτουργική απαίτηση. Ομοίως κάθε λειτουργική απαίτηση θα πρέπει να καλύπτει τουλάχιστον ένα στόχο ασφάλειας. Θα πρέπει να μπορεί να αποδειχθεί ότι ο συνδυασμός των επιμέρους λειτουργικών στοιχείων ικανοποιεί το δηλωθέντα στόχο ασφάλειας, ότι όλες οι απαιτήσεις είναι εσωτερικά συμπαγής, δηλαδή τα στοιχεία τους παρέχουν αμοιβαία υποστήριξη και ότι η δυναμικότητα των επιλεγμένων λειτουργιών είναι συνεπής με τους στόχους. Η κάλυψη μπορεί να αντικατασταθεί από μία τιμή: 0 καμία κάλυψη, 1 μερική κάλυψη, 2 πλήρης κάλυψη. Στην εικόνα 26 φαίνεται ο συγκεντρωτικός πίνακας που δημιούργησε το EBIOS με τις λειτουργικές απαιτήσεις όπου φαίνεται και ο βαθμός κάλυψης των στόχων ασφάλειας.

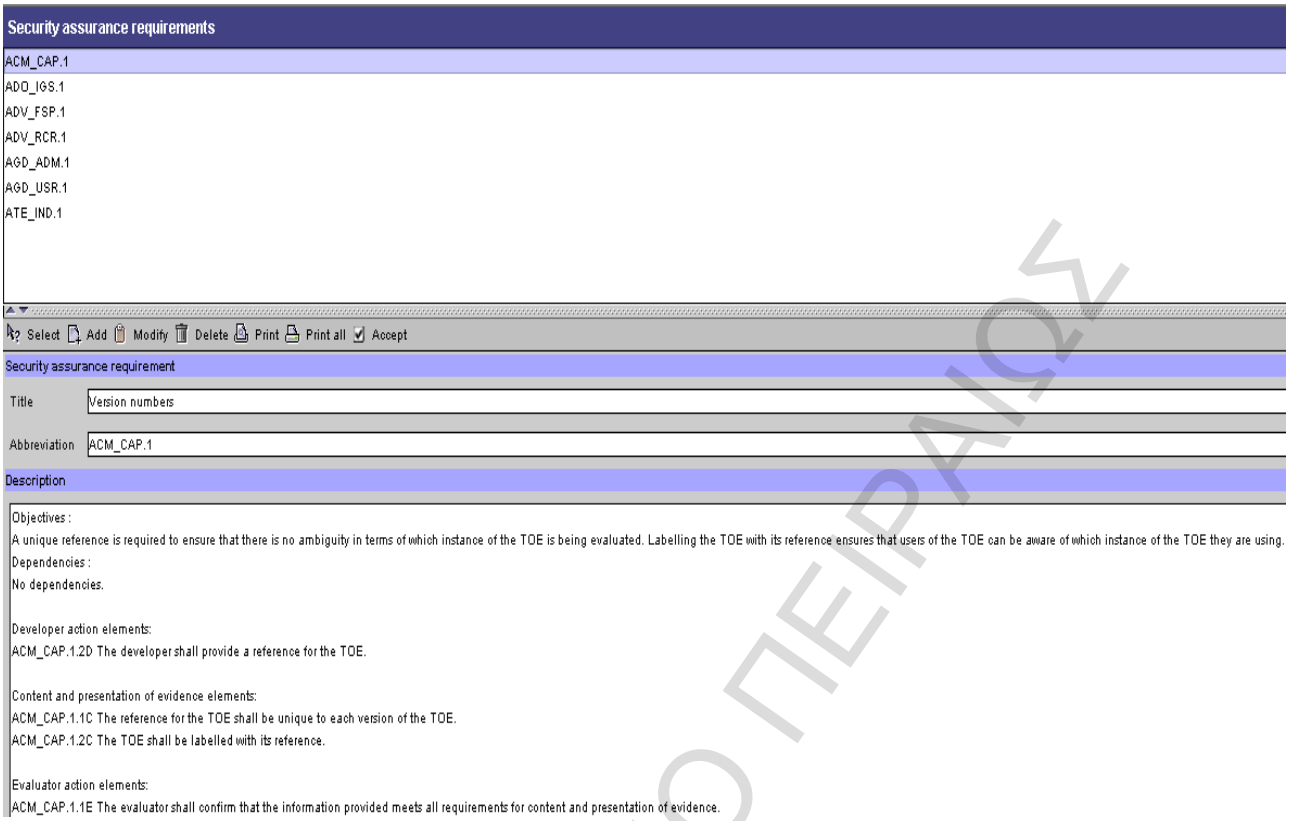
Coverage table

Security obje...	BCM_CLI.1.1	BCM_CLI.1.2	BCM_CLI.2.1	BCM_RLC.1.1	BCO_CEL.5.1	BCO_RPS.1.1	BCO_RPS.1.2	BCO_RPS.2.1	BDM_COC.1.1	BDM_COC.4.1	CIS_ADL.2.1	CIS_CDL.1.1	CIS_SSI.1.1	CIS_SSI.1.2	CPS_PPT.1.1	FAU_SAA.2.3	Coverage
O.LOG_03	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	1
O.LOG_08	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	2
O.LOG_11	☐	☐	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	2
O.LOG_12	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☑	2
O.LOG_13	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	2
O.MAT_03	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	2
O.MAT_07	☐	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	2
O.MAT_10	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	1
O.MAT_14	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	1
O.ORG_01	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	2
O.ORG_02	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	2
O.ORG_06	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☑	☐	2
O.ORG_10	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	2
O.ORG_11	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	1
O.ORG_26	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	2
O.ORG_27	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	2
O.PER_02	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	2
O.PER_03	☑	☑	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	2
O.PER_04	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	2
O.PER_05	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	2
O.PER_06	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	2
O.PER_08	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	2
O.PER_11	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	2
O.PHY_03	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	2
O.PHY_04	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☑	☑	☑	☑	☐	☐	2
O.RES_01	☐	☐	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	1
O.RES_02	☐	☐	☐	☐	☐	☐	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐	2
O.RES_06	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	1
O.TEST	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☑	☐	☐	☐	☐	☐	2
ORG_13	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	2
PER_13	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	2
ORG_22	☐	☐	☐	☐	☐	☑	☑	☑	☐	☑	☐	☐	☐	☐	☐	☐	2

Εικόνα 26. Συγκεντρωτικός πίνακας λειτουργικών απαιτήσεων-στόχων ασφάλειας.

4.5.2 Καθορισμός απαιτήσεων διασφάλισης (Δραστηριότητα 5.2)

Η διασφάλιση ότι οι στόχοι ασφάλειας επιτυγχάνονται με τις επιλεγμένες λειτουργίες ασφάλειας προκύπτει από δύο παράγοντες: α) την εμπιστοσύνη όσον αφορά τη σωστή υλοποίησή αυτών των λειτουργιών και β) την εμπιστοσύνη όσον αφορά την αποτελεσματικότητά τους. Οι απαιτήσεις αυτές μπορούν να ανήκουν στις εξής δύο κατηγορίες: α) σε αυτές που αφορούν το ίδιο το σύστημα και β) σε αυτές που αφορούν περιβάλλον του συστήματος. Όπως είπαμε στο προηγούμενο βήμα στη μελέτη μας επιλέξαμε το πρώτο επίπεδο διασφάλισης της λειτουργικής δοκιμής EAL 1. Η γνωσιακή βάση του EBIOS ορίζει αυτόματα τις απαιτήσεις διασφάλισης όπως φαίνεται στο παρακάτω στιγμιότυπο (Εικ. 27).



Εικόνα 27. Λειτουργικές απαιτήσεις για το επίπεδο EAL 1.

5. Συμπεράσματα – μελλοντικές επεκτάσεις

Βασικός στόχος της διατριβής ήταν η διενέργεια μίας μελέτης ανάλυσης επικινδυνότητας στο πληροφοριακό σύστημα μίας Βιβλιοθήκης Πανεπιστημίου. Για την επίτευξη αυτού του στόχου απαραίτητη ήταν η μελέτη του διεθνούς πρότυπου ISO/IEC 27002:2005 "Information technology – Security techniques – Code of practice for information security management" μέσα από το οποίο προτείνεται μία σειρά από βέλτιστες πρακτικές και διαδικασίες που έχουν ως στόχο την ασφάλεια της πληροφορίας μέσα σε έναν οργανισμό. Παράλληλα έχει αναπτυχθεί ένα πλήθος μεθοδολογιών και αντίστοιχων εργαλείων διεθνώς, για την υλοποίηση και διενέργεια αναλύσεων επικινδυνότητας στα πληροφοριακά συστήματα οργανισμών του δημοσίου και του ιδιωτικού τομέα, οι περισσότερες από τις οποίες βασίζονται σε αυτό το πρότυπο. Ύστερα από μία έρευνα μεταξύ των κυριότερων και πιο διαδεδομένων μεθοδολογιών επιλέχθηκε η EBIOS και το ομώνυμο εργαλείο.

Η μελέτη επικινδυνότητας του αυτοματοποιημένου πληροφοριακού συστήματος της Βιβλιοθήκης και Κέντρου Πληροφόρησης του Πρότυπου Πανεπιστημίου ανέδειξε μία σειρά από απειλές που αντιμετωπίζουν τα αγαθά – συστατικά του, οι οποίες εφόσον εμφανισθούν θα μπορούσαν να έχουν από μικρές μέχρι πολύ σοβαρές επιπτώσεις στην ορθή λειτουργία της βιβλιοθήκης και στην αδιάλειπτη παροχή υπηρεσιών στην ακαδημαϊκή κοινότητα. Οι απειλές αυτές αφού εντοπίσθηκαν και διατυπώθηκαν ξεκάθαρα, δημιούργησαν με τη βοήθεια του εργαλείου EBIOS στόχους ασφάλειας οι οποίοι θα πρέπει να καλυφθούν. Οι στόχοι αυτοί με τη σειρά τους, οδήγησαν στη διατύπωση συγκεκριμένων απαιτήσεων που θα πρέπει να καλύπτονται, για την εξασφάλιση της ασφαλούς λειτουργίας του πληροφοριακού συστήματος. Η μελέτη ανάλυσης που πραγματοποιήθηκε με το εργαλείο EBIOS καθώς και το περιληπτικό έγγραφο της μελέτης που εξάχθηκε αυτόματα από το εργαλείο συμπληρώνουν τη διατριβή.

Ως μελλοντική έρευνα προτείνεται η διενέργεια εκ νέου της μελέτης ανάλυσης επικινδυνότητας του πληροφοριακού συστήματος της ΒΚΠ, με κάποια άλλη από τις προτεινόμενες μεθοδολογίες, λόγου χάρη η CRAMM (η οποία διαθέτει αντίστοιχο εργαλείο επίσης), με στόχο τη σύγκριση των αποτελεσμάτων που προκύπτουν από τις δύο μεθοδολογίες. Για παράδειγμα η σύγκριση των απαιτήσεων ασφάλειας που προτείνει το EBIOS με τα αντίμετρα ασφάλειας που παράγει η CRAMM. Επίσης, ενδιαφέρον θα είχε η διενέργεια μίας μελέτης ανάλυσης επικινδυνότητας για ολόκληρο το πληροφοριακό σύστημα (Κέντρο Δικτύου) του Πανεπιστήμιο, υποσύστημα του οποίου θα μπορούσε να θεωρηθεί αυτό της ΒΚΠ. Βέβαια, σε αυτή την περίπτωση ελλοχεύει ο κίνδυνος κατάληξης σε μία εξαντλητική ανάλυση, με παραγωγή αποτελεσμάτων που δεν θα είναι εύκολα διαχειρίσιμα, εξαιτίας του όγκου της πληροφορίας. Τέλος, προτείνονται οι παρακάτω μελλοντικές επεκτάσεις της εργασίας, μιας και τα αποτελέσματα που προέκυψαν από το EBIOS αποτελούν εξαιρετική βάση για την υλοποίησή τους.

Δημιουργία Δήλωσης FEROS

Μετά την διεξαγωγή της ανάλυσης επικινδυνότητας με το εργαλείο EBIOS έχουμε μία πλήρη εικόνα του οργανισμού. Η ολοκληρωμένη μελέτη στο εργαλείο μπορεί να χρησιμοποιηθεί για την παραγωγή μίας Δήλωσης Ορθολογικής Έκφρασης των Στόχων Ασφάλειας (Rational Expression of Security Objectives Statement – FEROS). Η δήλωση FEROS είναι ένα έγγραφο που αφορά κυρίως συστήματα που χειρίζονται διαβαθμισμένη πληροφορία, αλλά μπορεί να εφαρμοστεί κατάλληλα και στα υπόλοιπα συστήματα. Πρόκειται για ένα έγγραφο το οποίο επισημοποιεί όλα τα στοιχεία που απαιτούνται προκειμένου ένας φορέας να εγκρίνει την εφαρμογή του συστήματος. Ως εκ τούτου, δεν περιγράφει μόνο το σύνολο των στόχων ασφαλείας και των κινδύνων που παραμένουν, αλλά και τη διαδικασία και το σκεπτικό που χρησιμοποιήθηκε για τον προσδιορισμό τους. Μετά την διεξαγωγή της μελέτης στο EBIOS, μπορούμε να εξάγουμε τα απαραίτητα δεδομένα (το εργαλείο παρέχει τη δυνατότητα εξαγωγής των δεδομένων σε html format), να αναδιοργανώσουμε του στόχους ασφάλειας (π.χ. να τους κατηγοριοποιήσουμε σε τεχνικούς και μη) και να προχωρήσουμε στη σύνταξη ενός FEROS.

Υλοποίηση πολιτικής πιστοποίησης

Μια πολιτική πιστοποίησης (**certification policy**) καθορίζει την πολιτική που πρέπει να εφαρμοσθεί από μία υποδομή δημοσίου κλειδιού (**public key infrastructure**), προκειμένου να διαχειριστεί πιστοποιητικά δημοσίου κλειδιού. Μόλις επισημοποιηθεί η πολιτική πιστοποίησης, μπορεί να χρησιμοποιηθεί ως βάση για τον καθορισμό συμφωνιών διαλειτουργικότητας μέσα από τη διαχείριση κλειδιών. Επίσης, μπορεί να χρησιμοποιηθεί κατά την παραγωγή δηλώσεων διαδικασιών πιστοποίησης, οι οποίες αντιπροσωπεύουν όλα τα τεχνικά και νομικά μέτρα, και τις μεθοδολογίες που χρησιμοποιούνται με στόχο τη συμμόρφωση στις απαιτήσεις ασφάλειας που προσδιορίσθηκαν στη πολιτική πιστοποίησης. Τα αποτελέσματα από τη διεξαγωγή της μελέτης ανάλυσης στο EBIOS μπορούμε να τα εξάγουμε και να τα χρησιμοποιήσουμε σε συνδυασμό με τον αντίστοιχο οδηγό, προκειμένου να παράγουμε μία πολιτική πιστοποίησης που να εφαρμόζεται στο σύστημά μας.

Δημιουργία προφίλ προστασίας

Ένα προφίλ προστασίας (**protection profile – pp**) είναι σύμφωνα με το διεθνές πρότυπο ISO/IEC 15408 – Common Criteria for IT Security Evaluations, ένα σύνολο από ισχύουσες απαιτήσεις για το σύστημα μελέτης, ανεξάρτητα από την εφαρμογή του, το οποίο ικανοποιεί συγκεκριμένες ανάγκες χρηστών. Πρόκειται για ένα έγγραφο με τυποποιημένο περιεχόμενο που μπορεί να χρησιμοποιηθεί ως μία προδιαγραφή με την οποία πρέπει να συμμορφώνεται ένας στόχος ασφάλειας. Αυτός ο στόχος προτείνει με αιτιολογημένη άποψη την κάλυψη των απαιτήσεων ασφαλείας που επίσημα ορίστηκαν στο προφίλ προστασίας. Τα προφίλ προστασίας θα πρέπει να είναι απόλυτα ολοκληρωμένα και συνεκτικά. Επομένως, θα πρέπει να παραχθούν με μεγάλη προσοχή, αλλά το πρότυπο δεν περιγράφει κάποια συγκεκριμένη μέθοδο. Η μελέτη που έχει διενεργηθεί στο EBIOS παρέχει όλα τα απαραίτητα στοιχεία για τη σύνταξη ενός προφίλ προστασίας διασφαλίζοντας παράλληλα τη συνέπειά τους.

Υλοποίηση στρατηγικού σχεδίου ασφάλειας ΠΣ

Το στρατηγικό σχέδιο για την ασφάλεια των ΠΣ (ISS master plan) είναι μία δήλωση της στρατηγικής ασφάλειας του οργανισμού υπό τους όρους της σχεδίασης, υλοποίησης και χρήσης ασφαλών ΠΣ για την επίτευξη της αποστολής και των στόχων του οργανισμού. Με τη μελέτη που ήδη διενεργήσαμε στο EBIOS παράγαμε μία δομημένη προσέγγιση η οποία βοηθάει σημαντικά στην δημιουργία του στρατηγικού σχεδίου.

Βιβλιογραφία

[1] Calder, A. and Watkins, S., *IT Governance, A Manager's Guide to Security and ISO27001/ISO27002*. London and Philadelphia: Kogan Page LTD., 2008.
[2] C. Albert and A. Dorofee "*OCTAVE Criteria, Version 2.0"* Software Engineering Institute, Carnegie Mellon University, Pittsburgh, Pennsylvania, Technical Report CMU/SEI-2001-TR-016, 2001. http://www.sei.cmu.edu/library/abstracts/reports/01tr016.cfm
[3] C. Albert, A. Dorofee and J.Allen, "*OCTAVE Catalog of Practices, Version 2.0*," Software Engineering Institute, Carnegie Mellon University, Pittsburgh, Pennsylvania, Technical Report CMU SEI-2001-TR-020, 2001. http://www.sei.cmu.edu/library/abstracts/reports/01tr020.cfm.
[4] Centers for Medicare & Medicaid Services – *CMS Information Security (IS) Plan of Action &Milestones (POA&M) Procedure,* Version 1.1, June 2009.
[5] Edward Humphreys, "Information security management standards: Compliance, governance and risk management," *Information Security Technical Report*, Volume 13, Issue 4, November 2008, pp. 247-255.
[6] European Network and Information Security Agency (ENISA), *Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools*, June 2006.
[7] Expression des Besoins et Identification des Objectifs de Sécurité (EBIOS) – SGDN/DSCSSI, *"MÉTHODE DE GESTION DES RISQUES"* (2010)
[8] Expression des Besoins et Identification des Objectifs de Sécurité (EBIOS) – SGDN/DSCSSI, *"ÉTUDE DE CAS @RCHIMED"* (2010)
[9] Expression des Besoins et Identification des Objectifs de Sécurité (EBIOS) – SGDN/DSCSSI, *"APPROACH",* Section 2, Version 2 (2004).
[10] Expression des Besoins et Identification des Objectifs de Sécurité (EBIOS) –SGDN/DSCSSI – *"TECHNIQUES"*, Section 3,Version 2 (2004).
[11] Expression des Besoins et Identification des Objectifs de Sécurité (EBIOS) –SGDN/DSCSSI – *"MEMO"* (2004).
[12] Federal Risk and Authorization Management Program (FedRAMP) – *Template and Process Quick Guide*, May 2012.
[13] ISO/IEC 27000:2005, *Information technology — Security techniques — Information security management systems — Overview.*
[14] ISO/IEC 27001:2005, *Information technology — Security techniques — Information security management systems — Requirements.*
[15] ISO/IEC 27002:2005, *Information technology — Security techniques — Code of practice for information security management*.
[16] J. Stuart Broderick, "ISMS, security standards and security regulations," *Information Security Technical Report*, Volume 11, Issue 1, 2006, pp. 26-31.
[17] Karin Höne, J.H.P. Eloff, "Information security policy — what do international information security standards say?," *Computers & Security*, Volume 21, Issue 5, 1 October 2002, pp.402-409.
[18] NATO/RTO, *Improving Common Security Risk Analysis – Final Report of Task Group IST-049, 2008.*
[19] National Institute of Standards and Technology Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, USA, July 2002.
[20] National Institute of Standards and Technology Special Publication 800-30 Revision 1, *Guide for Conducting Risk Assessments*, USA, September 2012.
[21] R. Caralli, J. Stevens, L. Young, and W. Wilson, "Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process," Software Engineering Institute, Carnegie Mellon University, Pittsburgh, Pennsylvania, Technical Report CMU/SEI-2007-TR-012, 2007. http://www.sei.cmu.edu/library/abstracts/reports/07tr012.cfm.

[22] SANS Institute InfoSec Reading Room, *An Introduction to Information System Risk Management*, July 2006.
[23] SANS Institute InfoSec Reading Room, *A Qualitative Risk Analysis and Management Tool – CRAMM*, Version 1.3, 2002. http://www.sans.org/reading_room/whitepapers/auditing/qualitative-risk-analysis-management-tool-cramm_83.
[24] Siemens - Management of Confidence – Insight Consulting – *Integrating Security into IT Projects and Programmes*, CRAMM v5.0.
[25] United States General Accounting Office – GAO, *Information Security Risk Assessment – Practices of Leading Organizations,* GAO/AIMD-00-33, November 1999.
http://www.gao.gov/special.pubs/ai00033.pdf

Σύνδεσμοι

[26] Agence nationale de la sécurité des systèmes d'information

[27] CCTA Risk Analysis and Management Method – CRAMM

[28] Computer Emergency Response Team – CERT

[29] European Network and Information Security Agency – ENISA

[30] National Institute of Standards and Technology

[31] WIKIPEDIA